UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA UNIVERSITARIA DE
INGENIERÍA TÉCNICA DE
TELECOMUNICACIÓN

CIBERDELINCUENCIA
DESARROLLO Y PERSECUCIÓN TECNOLÓGICA

Autor
Arturo Catá del Palacio

Tutor
Pedro Costa Morata

Septiembre 2014

PROYECTO FIN DE CARRERA
PLAN 2000

TEMA: Ciberdelincuencia. Desarrollo y persecución tecnológica.

TÍTULO: Ciberdelincuencia. Desarrollo y persecución tecnológica.

AUTOR: Arturo Catá del Palacio

TUTOR: Pedro Costa Morata **Vº Bº.**

DEPARTAMENTO: DIATEL

Miembros del Tribunal Calificador:

PRESIDENTE: Juan Blanco Cotano

VOCAL: Jesús Moreno Blázquez

Fecha de lectura: 30 de Septiembre 2014

Calificación: **El Secretario,**

Resumen

Cada día nos acercamos más a un mundo globalizado, en que Internet está marcando el paso. Este proyecto fin de carrera es una foto del estado actual de la ciberdelincuencia.

La ciberdelincuencia y el ciberdelito son conceptos que difieren depende de quién los defina, en este proyecto vemos algunas de estas definiciones y los diferentes tipos de ciberdelito. También intenta hacer un pronóstico razonado de lo que será el ciberdelito en los próximos años.

El proyecto hace un recorrido por la jurisprudencia y cómo los estados intentan luchar contra ella y ajustar su legislación al momento actual. Destacando además la problemática de perseguir delitos que se producen en distintos países y en los que en muchos casos el delincuente se encuentra en un país diferente de la víctima. Hace un recorrido por quien o puede ser víctima del ciberdelito, viendo como están aumentando las víctimas potenciales gracias a la gran penetración de Internet debida a la proliferación de los dispositivos móviles.

También cómo se están estableciendo mecanismos a nivel mundial de colaboración entre estados, tanto a nivel policial y judicial como de investigación y desarrollo.

Los ciberdelincuentes aprovechan las características implícitas de Internet, buscando ocultarse, por ello se dedica un capítulo de este proyecto a las principales redes de ocultación, conocidas como redes oscuras. En esta parte se hace especial hincapié en el uso de la red TOR, principal medio de ocultación a nivel mundial, y cómo funciona técnicamente, ya que sus definiciones y protocolos son conocidos al ser software libre.

Una vez conocido que ciberdelitos hay y como se producen, recorremos los distintos medios para la defensa y mitigación de los distintos ataques, esta parte del proyecto intenta desde un punto técnico acercarnos a lo que podemos hacer para defendernos, aunque algunos de los ataques son prácticamente imposibles de perseguir. Además de ver cómo defendernos de los posibles ataques dirigidos vemos cómo proteger las comunicaciones, a través principalmente, del cifrado de todo lo que enviamos a través de Internet.

Abstract

Every day we are moving to a global world, Internet is leading this change. This thesis end of grade is a picture of the current state of the cybercrime.

Cybercrime is a concept that differ depending on who is defining it. This document shows some of these definitions and the different types of cybercrime. Also it tries to make a reasoned forecast about the cybercrime in the near future.

The document run through the jurisprudence and how the states tries to adjust its legislation to the current moment. Emphasizing the problematic to prosecute crimes that are committed in different countries and crimes of which the cybercriminal is in a different country to the victim. In addition, the document define who may be a victim of cybercrime and how the number of potential victims are increasing because of the growth of the Internet penetration rate due to the proliferation of mobile devices.

Also it shows how the worldwide mechanisms are being established to collaborate among states on police and judicial context, and also on the research and development.

Cybercriminals exploit the characteristics of the Internet to hide from police, a chapter of this thesis talks about the nets known as darknets. This part emphasis on the use of the TOR network and how it works technically. TOR is the main net to communicate on the Internet anonymously. We can know how it works because it is free software and the specifications are public.

Once that we know how the cybercrime work and how many types are, we study the different ways to defense and mitigate the effects of attacks. In this part of the thesis we approach what we can do to defend our systems with technical perspective, even if some of attacks are impossible to pursue. Also, we explain how to keep our communications private, mainly though the encrypting methods when we transmit data over the Internet.

Agradecimientos

A mi familia por estar siempre ahí.

A Alberto, Patri, Isa y Rubén sin los que no lo habría conseguido.

A Nuria por su infinita comprensión.

ÍNDICE:

ÍNDICE DE FIGURAS

Acrónimos y abreviaciones

CCDFCOE - Centro de Excelencia para la Ciberdefensa Cooperativa

DNS – Domain Name Server

EDGE - Enhanced Data Rates for GSM Evolution

GNU – GNU is not Unix

GPL – General Public License

GSM – Global System of Mobile

HSPA – High Speed Packet Access

HTTPS - Hypertext Transfer Protocol Secure

ICMP – Internet Control Message Protocol

IETF - Internet Engineering Task Force

IDEA - International Data Encryption Algorithm

IGMP – Internet Group Management Protocol

IRC – Internet Relay Chat

LOPJ – Ley Orgánica del Poder Judicial

NCRP - National Central Reference Points

MAC - Message Authentication Code

MX – Mail Exchange Record

NAT – Network Access Translation

OCDE – Organización para la Cooperación y desarrollo económico

OTAN - Organización del Tratado del Atlántico Norte

OP – Onion Proxy

OR – Onion Router

PES - Proposed Encryption Standard

RFC – Request for Comments

SMTP – Simple Mail Transfer Protocol

SPF – Sender Policy Framework

TCP – Transmission Control Protocol

TTL – Time To Life

TOR - The Onion Router

UDP – User Data Protocol

VPN – Virtual Private Network

WCDMA - Wideband Code Division Multiple Access

WWW – World Wide Web

CAPÍTULO 1. INTRODUCCIÓN

1. Introducción

Aunque aparecen nuevo tipos de delito con el uso de las redes de comunicación, Internet no deja de ser un cambio de ámbito para delitos que, en su mayoría ya se estaban cometiendo, delitos como la pornografía infantil o los robos de datos han visto en Internet el lugar idóneo para su realización.

Internet ha supuesto un cambio de paradigma y una oportunidad para la delincuencia, ya que la facilidad de ocultarse y comunicarse en la red hace en muchos casos que el delincuente vaya por delante de las personas encargadas de hacer que las leyes se cumplan.

Las características de Internet son un quebradero de cabeza para los legisladores y técnicos que persiguen el ciberdelito, de la misma forma es una oportunidad para los delincuentes, Dan Jerker Savantesson (1) enumera las características de la red:

- Entorno sin fronteras
- Independencia geográfica
- Independencia de lenguaje
- Permite la comunicación de uno a muchos
- Sistema incomparable de distribución de la información
- Ampliamente utilizado, cada día más
- Portabilidad
- Falta de identificadores seguros
- Inexistencia de una autoridad central que controle el acceso a la WWW

La ciberdelincuencia es una preocupación para los estados, pero en la mayoría de los casos los delincuentes van por delante de los estados, las técnicas contra la ciberdelincuencia en muchos casos no son suficientes o no están bien implementadas por falta de expertos.

La red se ha convertido en un lugar para la ocultación de delitos clásicos y favorece la comunicación entre delincuentes.

(1) *Los cibercrímenes en el espacio de libertad, seguridad y justicia*. **Bernal, Antonio Pedro Rodríguez.** s.l. : Alfa-Redi, 2006, Revista de derecho informático Alfa-Redi.

1.1. Objetivos

El objetivo de este proyecto fin de carrera es intentar hacer una foto de la situación actual de la ciberdelincuencia, no pretende ser un documento técnico de referencia, aunque incluye gran cantidad de terminología y fundamentos técnicos sin los cuales no sería posible el estudio de este fenómeno y las formas en que se produce.

Esta foto global incluye una específica sobre la legislación mundial y cómo funciona en materia de delincuencia, intentando especialmente entender el funcionamiento a nivel mundial de la legislación y como los países, coaliciones y organismos colaboran entre ellos.

Otro de los objetivos es acercarnos a cómo son los delincuentes y como son capaces de ocultarse ante la ley haciendo hincapié en la parte más técnica del funcionamiento de las redes de ocultación.

Además intento acercar la gran cantidad de métodos que tenemos para defendernos de la ciberdelincuencia o mitigar las consecuencias de esta, la mayoría de ellos utilizados para evitar que nadie tenga acceso a nuestros sistemas y comunicaciones.

1.2. Estructura de la Memoria

En este documento podemos diferenciar dos partes, la dedicada a saber qué es y cómo y a quién afecta la ciberdelincuencia, que correspondería con los Capítulos 2 y 3 y una segunda parte más técnica en la que vemos como se ocultan los ciberdelincuente y que podemos hacer para defendernos de los ciberdelitos. A continuación vemos como está estructurado el documento y a qué está dedicado cada uno de los capítulos:

Capítulo 1. Introducción

Capítulo dedicado a los Objetivos del proyecto y la explicación de cómo se ha estructurado el documento.

Capítulo 2. Ciberdelincuencia

En este capítulo vemos de forma teórica que entendemos por ciberdelincuencia y ciberdelito. Que tipos de ciberdelincuencia y más concretamente de ciberdelitos existen y quienes son las víctimas de estos delitos.

También vemos quien nos defiende de los ciberdelincuentes y que hacen los principales organismos internacionales y uniones de países en materia de ciberdelincuencia y como se coordinan los distintos países.

En este capítulo vemos también el coste económico de la ciberdelincuencia y como se estima que será el futuro cercano de la ciberdelincuencia.

Como no podía ser de otra forma este capítulo hace un pequeño análisis de quienes son los ciberdelincuentes.

Capítulo 3. Jurisdicción en materia de ciberdelincuencia

La jurisdicción es uno de los puntos más complejos cuando hablamos de ciberdelincuencia, en este capítulo haces un análisis básico de como está ahora mismo la ciberdelincuencia, la complejidad de legislar algo que sucede internacionalmente.

En este capítulo dedico un gran esfuerzo al análisis del Convenio Europeo sobre Ciberdelincuencia, ya que se trata del documento más importante a nivel mundial en la materia y es referencia en todos los avances legislativos mundiales.

Capítulo 4. Técnicas Usadas en el cibercrimen

Este capítulo está dedicado al estudio de la forma de moverse de los criminales en la red, especialmente de sus métodos de ocultación.

El peso importante del capítulo se dedica a la red TOR, a que es y sobre todo como funcionan sus protocolos, que se ha convertido en el estándar a la hora de ocultarse para cometer delitos. Además se analizan la red Freenet, de gran importancia en el intercambio ilegítimo de ficheros.

La última parte del capítulo está dedicada a un pequeño supuesto práctico que consiste en conectarse a la red TOR y navegar por Internet, demostrando lo fácil que resulta.

Capítulo 5. Técnicas usadas en la defensa y seguimiento del cibercrimen

Este es el capítulo más técnico del documento, en el podemos ver técnicas de defensa para proteger nuestros datos y comunicaciones, detallando en muchos casos los procedimientos de ataque más comunes y las acciones que se pueden hacer para mitigarlos o evitarlos. Hablo de las herramientas más comunes para asegurar nuestras redes y comunicaciones.

Capítulo 6. Conclusiones

Pequeño resumen de lo aprendido en la realización de este documento.

Capítulo 7. Bibliografía.

Listado de documentos consultados para realización de este documento.

CAPÍTULO 2. CIBERDELINCUENCIA

2. Ciberdelincuencia

2.1. ¿Qué es?

La ciberdelincuencia es compleja de definir, porque no hay consenso y probablemente nunca lo habrá como con otros delitos comunes, sobre lo que es un ciberdelito. Ni siquiera con la formar de referirnos, en muchos textos veremos que se habla indistintamente de ciberdelito, delito informático (computer crime), cibercrimen, delitos cometidos a través de sistemas informáticos, delitos telemáticos, etc.

Cuando hablamos de delito informático, son varios organismos los que poseen una definición.

La ITU[1] define ciberdelito como: "*Un delito informático (computer-related crime) es aquél cuyo objeto o medio de realizarlo es un sistema informático, está relacionado con las tecnologías digitales y se integra en los propios de la delincuencia de cuello blanco. El ciberdelito (cybercrime) es una forma del delito informático que recurre a las tecnologías de Internet para su comisión, refiriéndose por tanto a todos los delitos cometidos en el ciberespacio."* (2).

Por su parte la OCDE en 1983 hablaba de infracción informática: "infracción informática como todo comportamiento ilegal, inmoral o no autorizado que afecta a la transmisión o al procesamiento automático de datos." (2).

La Commonwealth define el "delito relativo a los sistemas de cómputo" como un "acto criminal en el que el objetivo es un sistema informático".

El no haber una definición aceptada, parece un pequeño problema, ya que en la mayoría de los casos son definiciones similares, que incluirían los mismos tipos de delito. Pero sigue habiendo una gran discusión sobre que es ciberdelito y lo que no. Esto es un gran problema en el ámbito jurídico, que obliga prácticamente a desarrollar un listado de delitos que estarían definidos como delito en cada documento o ley formulada, ya que el hecho de no haber consenso puede generar muchos problemas con las leyes como veremos en el punto 3.1.

(2) **Unión Internacional de Telecomunicaciones.** *Guía de Ciberseguridad para los Paises en Desarrollo.* [http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf] 2007.

[1] Unión Internacional de Telecomunicaciones, UIT en español.

Como vemos podemos hablar de ciberdelincuencia en dos supuestos:

- El delito es cometido a través de un sistema informático
- El objeto del delito es un sistema informático

2.2. Tipos

Definir tipos de delitos vuelve a ser una tarea compleja, hay muchas formas en las que podríamos dividirlos, como podría ser la gravedad, a quien afecta, etc. pero en este caso nos hemos fijado en la división que establecen dos organismos tan importantes como son la ONU y la el Consejo de Europa.

La ONU establece tres tipos de Delito Informático:

- Fraudes cometidos mediante manipulación de computadoras
- Manipulación de los datos de entrada
- Daños o modificaciones de programas o datos computarizados

Esta división parece que se queda un poco corta, ya que no llega a contemplar todos los supuestos, por lo que vamos a usar la que establece el Consejo de Europa.

El Convenio sobre Ciberdelincuencia del Consejo de Europa (3) establece una división de los delitos informáticos en el que distingue cuatro tipos: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, delitos informáticos, delitos relacionados con el contenido y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Aunque altamente aceptada esta división debido a la gran variedad de delitos puede hacer que los delitos puedan estar incluidos en varias categorías, o que incluso podamos llegar a la conclusión de que nuevos delitos aparecidos desde 2001 como el phising sean difíciles de categorizar.

(3) **Europa, Consejo de.** Convenio Europeo de Ciberdelincuencia. Budapest : s.n., 2001.

2.2.1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

El grueso de los delitos que se producen tiene como víctima un equipo informático y datos informáticos. Estos delitos incluyen:

Acceso Ilícito: son los considerados comúnmente como piratería, y se refieren al acceso no autorizado en un sistema, "infringiendo las medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva". (3)

Dos ejemplos sencillos de este tipo de delito sería el acceso a sitios web protegidos por contraseña o el acceso a equipos protegidos con contraseña.

Para realizar este tipo de delitos se puede utilizar software específico para romper una contraseña, por ejemplo, a través de un ataque por fuerza brutas. Para conseguir la contraseña también se utilizan sitios web falsos o malware[2] capaz de guardar los datos de acceso del usuario.

Interceptación Ilícita: la interceptación de una comunicación legítima por medios técnicos en transmisiones no públicas que se producen entre sistemas informáticos. Esto incluye las emisiones electromagnéticas provenientes de sistemas informáticos.

Para hacer esto los delincuentes atacan la infraestructura de comunicaciones, tanto fijas como inalámbricas. Esto incluye comunicaciones "clásicas" y a través de Internet.

Es uso de redes inalámbricas públicas puede poner muy fácil la interceptación de datos para los delincuentes.

Ataques a la Integridad de los Datos: se considera ilegítimo que se "dañe, borre, deteriore, altere o suprima datos informáticos". (3)

Una manera muy común de realizar este tipo de delito es a través de malware, este tipo de software cada vez es más avanzada y difícil de detectar.

Ataques a la Integridad del Sistema: se considera un delito la alteración de un sistema informático, obstaculizando el funcionamiento mediante la transmisión de datos.

(3) **Europa, Consejo de.** Convenio Europeo de Ciberdelincuencia. Budapest : s.n., 2001.

[2] Ver punto 5.4

Muchas legislaciones están incorporando este tipo de delito, que incluye dejar fuera de línea un servicio concreto, como puede ser una página web.

Para hacer este tipo de ataques se utiliza malware, y ataques de denegación de servicio[3].

Abuso de los Dispositivos: el Convenio sobre Ciberdelincuencia sugiere tipificar como delito la creación de herramientas que faciliten otros tipos de delito. Así como la distribución de datos de acceso a otros sistemas.

Se puede considerar delito simplemente la posesión de este tipo de herramientas.

2.2.2. Delitos informáticos

Falsificación informática: se considera delito la modificación, introducción, borrado o eliminación de datos legítimos. El uso de datos falsos buscando que sean tomados por verdaderos es considerado delito.

Fraude Informático: este tipo de delito es muy común en Internet, se considera que el uso de datos falsos que causen perjuicio patrimonial a otra persona es delito, también cualquier interferencia en el funcionamiento que cause el mismo perjuicio está tipificado de la misma manera.

La mayoría de los fraudes de este tipo son considerados fraudes de carácter común y no delitos informáticos, aunque se hayan usado medios electrónicos para cometer el delito.

También es un delito el robo de identidad, sea cual sea el medio.

Entra dentro de este tipo de delitos la falsificación informática, como puede ser la alteración o falsificación de un documento por medios electrónicos o la manipulación de imágenes con intención dolosa.

[3] Ver punto 5.3

2.2.3. Delitos relacionados con el contenido

Esta categoría responde al uso de Internet para compartir documentos con contenido ilícito, en todos los casos este tipo de contenido fuera de la red sería delito de la misma forma que a través de la red.

El problema de este tipo de delito es que no es fácil de llegar a un acuerdo para legislar a nivel mundial, ya que en algunos países lo que es tipificado como delito en un país en otros se considera libertad de expresión. Esto ocurre por ejemplo con el material xenófobo.

Delitos relacionados con Pornografía Infantil: al contrario que en la pornografía para adultos, que hay diversidad de legislaciones, con la pornografía infantil hay unanimidad en la condena y normalmente se consideran actos criminales. Además del Convenio Europeo de Ciberdelincuencia tenemos varias organizaciones que luchan para la erradicación de este tipo de contenido, como al Convención de las Naciones Unidas sobre los derechos del Niño de 1989, la Decisión Marco del Consejo de Europa relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil de 2003, el Convenio sobre Protección de los niños contra la explotación sexual y el abuso sexual del Consejo de Europa de 2007 y un largo etcétera.

Se estima que la utilización de divisas virtuales como Bitcoin y de tecnologías de cifrado y redes oscuras[4] favorece este tipo de delito.

Los siguientes delitos no se contemplan en el Convenio Europeo sobre Ciberdelincuencia de 2001, pero esto se corrige con el Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos de 2003. (4) (Europa, 2013)

Por material racista y xenófobo se entiende “todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión” (4)

Delitos relacionados con la difusión de material racista y xenófobo: la compartición de ficheros o información que se considere material racista será considerado delito.

(4) **Europa, Consejo de.** *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.* 2013. 261/05/CON.

[4] Ver punto 4

Delitos relacionados con insultos o amenazas con motivación racista y xenófoba: la compartición de ficheros o información que contengan insultos o amenazas con motivación racista y xenófoba será considerado delito.

Delitos relacionados con la negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad: la negación, minimización burda, aprobación o justificación de genocidio o de crímenes contra la humanidad "tal como se definen en el derecho internacional y reconocidos como tales por una decisión definitiva y vinculante del Tribunal Militar Internacional" (4) será considerado delito.

Aunque no se contemplan como tal en el Convenio sobre Ciberdelincuencia del Consejo de Europa, también es considerado delito en múltiples jurisdicciones solicitar o incitar a un crimen, la venta ilegal de productos y dar información e instrucciones para actos ilícitos, como podría ser la construcción de explosivos o la fabricación de droga.

2.2.4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Delitos relacionados con Infracciones de la propiedad Intelectual y de los derechos afines: las empresas utilizan Internet para comunicar información y poner a disposición de sus clientes los productos. En la red se pueden encontrar problemas similares a las falsificaciones de fuera de la red, con el añadido de que la falsificación puede ser realmente exacta al producto original.

Con el desuso de los soportes físicos y la digitalización de la industria de la propiedad intelectual se ha convertido en un verdadero quebradero de cabeza el mantener fuera de las redes de compartición de ficheros el contenido digitalizado.

Las infracciones de derechos de autor más comunes son el intercambio en sistemas de intercambio de archivos de programas informáticos y archivos multimedia con copyright.

El uso ilegal de marcas para actividades delictivas y los delitos en materia de dominios y nombres también son un delito a perseguir en la red.

(4) **Europa, Consejo de.** *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.* 2013. 261/05/CON.

2.3. *Víctimas de la ciberdelincuencia*

2.3.1. Individuales

Como ya hemos comentado, la ciberdelincuencia no sólo afecta a las personas conectadas a la red, ya que esta es usada como el medio y como el fin, es decir, los delincuentes pueden usar la red para sus comunicaciones y transacciones, en este caso Internet sería un **medio** de comunicación más, que facilita la ocultación y estar en cualquier punto del mundo de alguna forma.

Por otra parte, están los delitos propios de la red, como pueden ser los ataques a sistemas conectados, el ciberacoso, suplantación de identidad, etc. En este caso serían las personas o entidades conectadas a Internet las que podrían ser víctimas. Con los cambios en la forma de utilizar la red en los últimos a años, con cada vez más datos personales compartidos hacen que los particulares (redes sociales, WEB 2.0) y los datos que estos aportan sean cada vez más perseguidos por los ciberdelincuentes.

A nivel mundial cada día estamos más conectados, el ciberespacio se puede considerar cada vez un medio más colectivo y popular, acceder a un terminal con acceso a Internet cada día es más fácil y barato. En el siguiente mapa vemos el índice de penetración de Internet en 2013, con datos del banco mundial (5):

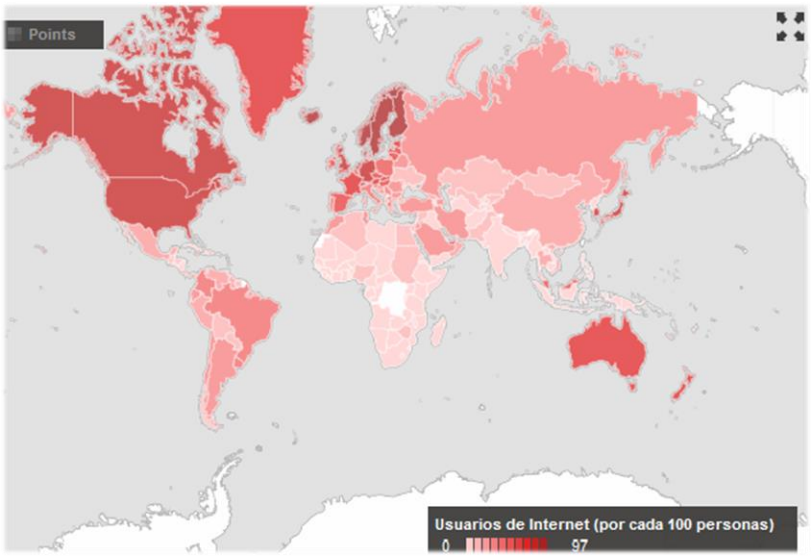

Figura 1. Índice de penetración de Internet.

(5) **El Banco Mundial.** El Banco Mundial BIRF-AIF. *Usuarios de Internet (por cada 100 personas).* [En línea] 2013. http://datos.bancomundial.org/indicador/IT.NET.USER.P2 /countries?page=2&display=map.

Como vemos en el mapa anterior, en los países más desarrollados el uso de Internet está cada vez más cercano a toda la población. Con el paso de los años se reduce la brecha digital y cada vez hay menos gente conectada, todas estas personas pueden ser víctimas de una u otra forma del ciberdelito en Internet, al igual que en otro tipo de delitos fuera de la red, las personas con menos formación específica son más propensas a ciertos tipos de delito, por ejemplo en el caso del Phising[5].

El acceso a Internet a través del móvil ha hecho que aumente el número de personas conectadas, sobre todo en segmentos de la población que antes no llegaba Internet. Actualmente hay más de 1,2 billones de líneas móviles, lo que supone que el 16% de la población mundial.

El informe de Norton de 2011 (6) indica que se producen 431 millones de ataques, lo que supone un millón diario de víctimas.

Este mismo informe indica que el 10% de los adultos ha sufrido un ataque a través de su teléfono móvil, incluyendo un nuevo fenómeno llamado smishing que consiste en phising a través de SMS. Es precisamente el phising el que ocupa el tercer puesto entre los cibercrímenes. En segundo lugar tenemos las estafas online.

(6) **Norton Symantec.** *Informe sobre el cibercrimen Norton.* 2011.

[5] El phising consiste en la suplantación de la identidad de un tercero. Este tipo de abuso se usa para robar usuarios, contraseñas, números de tarjeta, etc. Su funcionamiento es sencillo, se envía al usuario por correo electrónico, mensajería instantánea, sms, etc, un enlace que simula ser un sitio conocido para engañar al usuario y que este introduzca sus datos.

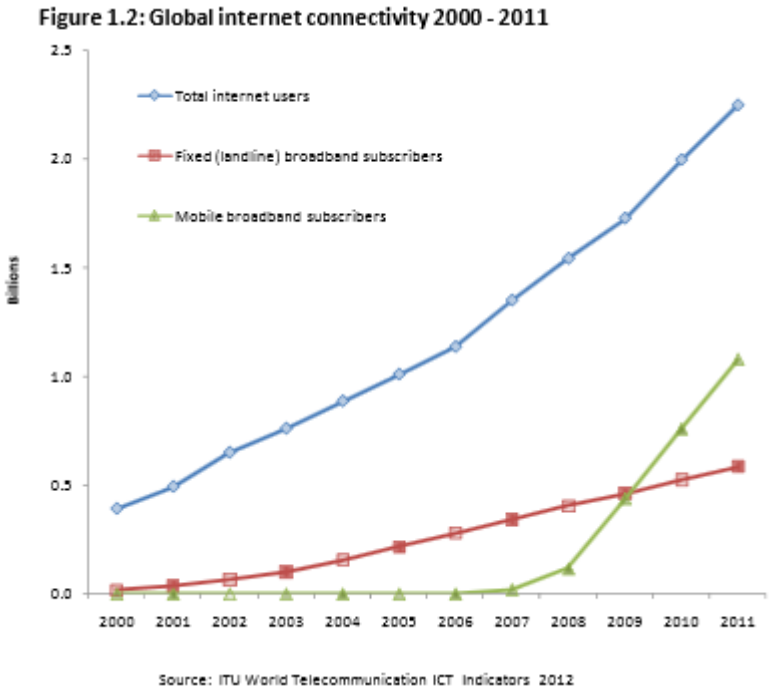

Figura 2. Comparativa entre el número total de accesos a Internet y los accesos a través de móviles. (7)

Este mismo informe estima que en 2017 el 90% de la población mundial podrá tener acceso a una línea móvil GSM/EDGE, con el 85% de esta población accediendo a líneas móviles de alta velocidad WCDMA/HSPA.

Como vemos millones de personas pueden ser víctimas de la ciberdelincuencia sólo por el hecho de estar conectados a la red.

Se han dado casos muy sonados de ataques individuales, como el sucedido en agosto de 2014, en el que 100 mujeres famosas fueron víctimas de un ataque dirigido para robar las imágenes que estas almacenaban en sus teléfonos móviles o en el servicio online de almacenamiento iCloud. En este caso los ataques han utilizado un fallo en la seguridad de este sistema que ha permitido la realización de un ataque de fuerza bruta para robar las contraseñas de sus usuarios. El código del software atacante ha llegado a estar disponible en github[6]. O el robo del número de la tarjeta de crédito de Bill Gates por un galés de 19 años en 2001.

(7) **United Nations Office on Drugs and Crime.** *Comprehensive Study on Cybercrime.* Viena : s.n., 2013. UNODC CCPCJ EG.4.

[6] Github es una herramienta online de gestión de versiones usada en el desarrollo de software.

2.3.2. Menores

Principalmente hay dos delitos que afectan de una manera importante a menos, estos son la **pornografía infantil** y el **ciberacoso** (que también afecta a personas de todas las edades, pero de una manera más importante a los menores). Otros tipos de delito pueden afectar a los menores como a cualquier usuario de Internet.

Pornografía Infantil:

UNICEF afirma que en 2011 había más de 16.000 (el año anterior había poco más de 10.000) sitios web de pornografía infantil en Internet, esto supone que decenas de miles de niños son víctimas de abusos que luego son transmitidos a través de la red. (8)

UNICEF afirma que es prácticamente imposible eliminar los riesgos del ciberespacio, por lo que afirma hay que "eliminar la impunidad de los abusadores, la reducción de la disponibilidad y el acceso, así como el apoyo a la recuperación de las víctimas." (8)

Hay que prevenir el acceso sin preparación de los menores a la red, y sobre todo educarles para hacer buen uso y evitar que el uso de Internet favorezca que se cometan abusos, ya que es prácticamente imposible conseguir que no se compartan los ficheros.

Ciberacoso (Ciberbullying):

El ciberacoso es la utilización de los sistemas de información para acosar, amenazar, avergonzar o causar daño de una u otra forma a una persona. Para este tipo de acoso se utilizan medios como la mensajería instantánea en el móvil, las redes sociales, el email, etc.

Lo normal es que sean las mismas víctimas de acoso tradicional (verbal, físico) las que sean víctimas del ciberacoso. INTECO afirma que el 5% de los menores es víctima de ciberacoso en España. (9)

Cuando hablamos de acoso de un adulto a un menor, se ha acuñado el término **Grooming**, que consiste en establecer una relación de confianza con el menor, para conseguir control sobre este. Normalmente se utiliza este control para abusar de los menores, ya sea físicamente o para por ejemplo conseguir fotos de los menores de naturaleza sexual.

(8) **Unicef.** *Seguridad infantil en Internet: retos y estrategias mundiales.* 2011.

(9) **INTECO.** *El ministro de Industria, Energía y Turismo presenta una campaña contra el ciberacoso infantil.* 2013.

2.3.3. Empresas

Hoy en día las empresas utilizan Internet a diario para la obtención de información, teletrabajo, ventas directas, contactos entre proveedores y clientes y realización de operaciones financieras y trámites administrativos.

A día de hoy casi todas las empresas tienen acceso a Internet y cada vez más por lo menos en los países más desarrollados, en España las cifras son cada vez más cercanas al 100%

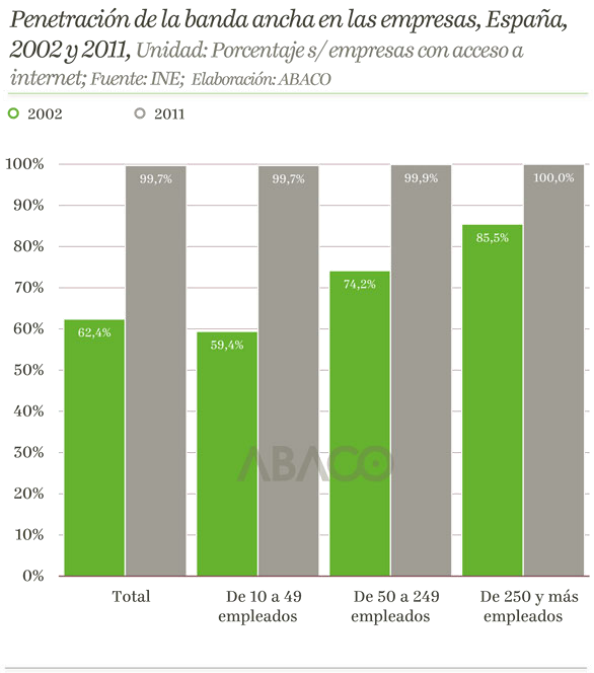

Figura 3. Penetración de acceso a Internet en empresas españolas. (10)

Las empresas pueden ser víctimas de ciberespionaje, de robo de información y de ataques que afecten a su productividad o ventas.

Ciberespionaje industrial: se habla de ciberespionaje industrial a la obtención por medios ilícitos de la información relativa a la investigación, desarrollo y fabricación de prototipos. Con este tipo de robo se busca adelantarse a los competidores, normalmente este tipo de robos los realizan las propias empresas, aunque en algunos casos hay delincuentes que se dedican a este tipo de robos para luego vender los datos a terceras personas.

Además de estos robos, en los últimos años se ha acusado a China de robar miles de documentos de empresas de todo el mundo con el fin de favorecer a sus empresas.

(10) **Observatorio ABACO.** Penetración de internet (empresas). [En línea] http://www.observatorioabaco.es/post_observatorio/penetracion-de-internet-empresas.

Robo de información: en muchas ocasiones se realizan robos de información, esta puede ser muy diversa, como ya hemos visto en el punto anterior puede tener un carácter industrial, pero también es normal robar datos de carácter personal, como puede la cartera de clientes o proveedores de una empresa.

Ataques: las empresas en muchas ocasiones son víctimas de ataques que buscan dejar fuera de servicio sus comunicaciones. Esto puede afectar gravemente a su negocio, por ejemplo la caída de una tienda online puede generar millones en pérdidas. Normalmente este tipo de ataques son ataques de Denegación de Servicio[7].

Robos de dominios: aunque este tipo de delito puede afectar también a estados y personas, es en el mundo de las empresas donde adquiere más importancia este tipo de delito. Los delincuentes adquieren los dominios y se dedican a venderlos a los que en principio serían los usuarios legítimos ya que son propietarios del nombre de la marca. Además de este tipo de robos de dominios hay un tipo de dominio que se denomina Typosquatters y que son lo suficientemente parecidos al dominio legítimo como para llegar a confundir al usuario y ser utilizados de forma ilegítima. Un ejemplo de este tipo de dominio sería www.goggle.com que durante mucho tiempo se ha dedicado a suplantar a www.google.com e infectar a los usuarios cuando realizan búsquedas.

2.3.4. Estados

Ciberespioaje y ciberguerra: durante años se acusado a EEUU de ciberespionaje y de usar la red echelon para interceptar las comunicaciones, con el escándalo de Wikileaks[8] ha quedado demostrado que estas interceptaciones se están produciendo, incluso en las comunicaciones de sus aliados como Alemania.

Las revelaciones de Snowden en 2013 han puesto en alerta a muchos países, que han visto como EEUU les estaba investigando y monitorizando. Durante muchos años ha sido EEUU quien ha acusado y puesto en el disparadero a China por su ciberespionaje.

[7] Ver punto 5.3

[8] Wikileaks es una organización sin ánimo de lucro que ha publicado en los últimos años gran número de documentos filtrados. Su actividad comienza en 2007, desde entonces ha filtrado más de un millón de documentos, algunos de los cuales han tenido gran impacto, como los relativos a las guerras de Afganistán e Irak y gran cantidad de Documentos de Estado de EEUU.

Ciberguerra: cuando hablamos de ciberguerra, hablamos del desplazamiento de un conflicto al ciberespacio y las tecnologías de la información. También se considera ciberguerra a las alteraciones en la información y sistemas del enemigo y a la protección de los propios.

Richard A. Clarke define ciberguerra como: "Se denomina ciberguerra cualquier penetración no autorizada por parte de, en nombre de, o en apoyo a, un gobierno en los ordenadores o las redes de otra nación, en la que el propósito es añadir, alterar o falsificar información o causar años a, o perturbar el adecuado funcionamiento de, un ordenador, un dispositivo de red o los objetos controlados por el sistema informático" (11)

Se da la circunstancia de que no hay acuerdo internacional sobre el conflicto en este terreno, por lo que se percibe como un escenario de impunidad. El único documento de referencia del que se dispone en este momento es el conocido como "Manual de Tallín", que ha sido elaborado por el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN. Este manual recoge por un lado como el derecho internacional puede aplicarse a la ciberdefensa en la OTAN y por otro establece 95 normas que deberían cumplirse en este tipo de conflictos. Está realizado por un grupo de expertos y no recoge la opinión de la OTAN.

A finales de marzo de este año (2014), el Departamento de Defensa de Estados Unidos detallaba su prepuesto, en el que la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) dispondrá de 3.000 millones de dólares para investigación, esta agencia tiene una gran parte de su investigación relacionada con Internet. Durante las guerras de Irak y Afganistán las Fuerzas Armadas de EEUU han utilizado avances en la materia desarrollados por esta agencia. DARPA se encuentra desarrollando en este momento el programa de guerra cibernética conocido como Plan X, que está pensado para "*tecnologías revolucionarias para la comprensión, la planificación, gestión y ejecución de la ciberguerra en tiempo real, a gran escala y en entornos de red dinámicas".*

El ministro de defensa francés, ha anunciado un presupuesto de 1.500 millones de euros para el periodo 2014-2016 para mejorar la resiliencia de sus sistemas TIC y sus capacidades de ciberdefensa y ciberseguridad.

(11) **Clarke, Richard A.** *Guerra en la Red. Los Nuevos Campos de Batalla.* Barcelona : Ariel, 2011. ISBN 9788434469600.

Cada vez tiene más presencia entre los expertos en seguridad el término “ciberguerra fría”, esta ciberguerra fría se estaría produciendo en los últimos años entre Estados Unidos y China. Como ocurrió en la guerra fría, la ciberguerra fría se ha convertido en una carrera tecnológica, en la que ambas partes incrementen sus capacidades defensivas y ofensivas. Se han publicado informes que demuestran la participación del Ejército Popular de Liberación Chino a través de su unidad de ciberinteligencia en ataques para rastrear los sistemas estadounidenses, especialmente de empresas y organismos cuya información pueda ayudar al Gobierno de China en su crecimiento estratégico (nuevas energías, biotecnología, nuevos materiales, seguridad de red, industria aeroespacial, industria de comunicaciones). En mayo de 2007 se produjo uno de los ataques más importantes, con el acceso de ciberespías a diseños del sistema de defensa de EEUU como afirma el Washington Post. (12)

En la documentación filtrada por Edward Snowden en 2013 se detalla una operación contra el gigante chino de las comunicaciones Huawei que pretendía demostrar la relación entre esta y el Ejército Popular de Liberación chino.

En los últimos años han tenido lugar varias cumbres bilaterales entre EEUU y China en las que el ciberespionaje ha tenido un lugar destacado.

Ciberterrorismo: es un hecho que hay día de hoy los ciberterroristas van por delante de la mayoría de los estados. Por ello las principales potencias en materia de guerra, como son Estados Unidos, Reino Unido, Francia e Israel están poniendo en marcha la creación de unidades de ciber-reservistas. Por ejemplo, el gobierno israelí ha creado una unidad de más de 8.000 efectivos perteneciente al Cuerpo de Inteligencia De las Fuerzas de Defensa de Israel, estos ciber-reservistas están repartidos a lo largo del mundo. Se considera que todos los países necesitan una Estrategia de Ciberseguridad Nacional, que aglutine ámbitos como la investigación y desarrollo en materia de seguridad, legislación y formación.

Normalmente el objetivo de los ciberterroristas son las redes de suministro (agua, electricidad, gas, etc.), las redes de comunicación, los sistemas de satélite, los ordenadores de organismos y ministerios de seguridad. Este tipo de ataques normalmente tiene como objeto la presión al estado en una determinada causa no legítima, escudada normalmente en ideologías políticas y religiosas.

(12) **Nakashima, Ellen.** The Washington Post. *Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies.* [En línea] 27 de Mayo de 2013. http://www.washingtonpost.com /world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

Por ciberterrorismo entendemos el uso de medios informáticos y tecnologías de la información para generar terror o miedo. Algunos autores hablan del ciberterrorismo como "la convergencia del ciberespacio con el terrorismo".

Ciberactivismo: cuando hablamos de ciberactivismo hablamos del conjunto de técnicas y tecnologías basadas en Internet y la telefonía móvil. Aunque el activismo como tal no es un problema, muchas acciones de ciberactivismo acaban en acciones colectivas y en lo que se conoce como hacktivismo. Esta unión de hacker y activismo ha generado en muchas ocasiones problemas a organizaciones y gobiernos, la forma más común de generar problemas por estos activistas cibernéticos son los ataques de denegación de servicio (ver punto 5.3) o las modificaciones de páginas web para incluir los mensajes de la reivindicación. En alguna ocasión han llegado a robar y publicar datos confidenciales.

El que se estima que es el primer caso de hacktivismo data de 1989 cuando máquinas de la NASA fueron penetradas por el gusano informático WANK y cambió el mensaje de entrada al sistema. En los últimos años ha habido multitud de actos de este tipo, algunos contra organismos gubernamentales tan importantes como la NSA estadounidense en los 1999 y 2000, concretamente contra su red de espionaje Echelón.

Dentro del movimiento hacktivista hay un grupo que se ha convertido en el principal protagonista de la red: **Anonymous**.

Anonymous es un grupo de individuos anónimos que actúan sin jerarquía ninguna, se han convertido en el adalid de la libertad de Internet, la neutralidad y la libertad de expresión. La mayor parte de sus acciones han sido buscando el bloqueo de páginas web, pero entre sus acciones también encontramos robos y publicación de información secreta y manifestaciones.

Alguno de sus miembros ha sido detenido acusado asociación ilícita y por administrar los chat desde los que se ha organizado alguno de los ataques.

2.4. Quién comete los ciberdelitos

Como en todos los delitos, hablar de un perfil en complejo, pero estadísticamente se ha llegado a elaborar un perfil típico del delincuente en Internet. Estas son las características comúnmente aceptadas y plasmadas por Javier A. Díez en su *Perfil de un Hacker* (13):

(13) **Diez, Javier A.** Perfil de un Hacker. [En línea] http://www.derechopenal.unican.es/contenido/hackers.pdf.

- Varón
- De 12 a 28 años
- Clase Media
- Obsesivo
- Problemas familiares
- Solitarios
- Adicción a los ordenadores
- Con un mínimo de conocimientos técnicos
- Complejo de inferioridad

Como hemos comentado anteriormente podemos considerar que la red es el medio o el fin, en este caso vamos a hablar de los tipos de delincuentes que cometen delitos propios de Internet. En general y de forma en muchos casos errónea se usa el término Hacker para definir este tipo de delincuentes.

En el código penal español no hay una clasificación de ciberdelincuentes por lo que en general se usan las clasificaciones que se hacen en Internet, a continuación detallamos los tipos de delincuentes en función de sus conocimientos y motivaciones, creado por Marcus Rogers de la Universidad de Purdue en Indiana:

Principiante: posee conocimientos limitados, simplemente se dedica a usar las herramientas disponibles, no desarrollando nada. Saben usar las herramientas, pero no como funcionan ni sus consecuencias. Buscan atención mediática.

Codificadores: son los encargados de desarrollar las herramientas que posteriormente son usadas por los principiantes. Su motivación en general es la de adquirir prestigio.

Cyber-punks: al igual que los codificadores se encargan de desarrollar el software que utilizan. Conocen perfectamente cómo funcionan los ataques y los sistemas que atacan. Se les achacan robos de tarjetas de crédito y numerosos fraudes. Les gusta dar a conocer sus ataques.

Hackers de la vieja guardia: no tienen una intención criminal pero no respetan las leyes. Especialmente las relacionadas con la propiedad. Les interesa la superación intelectual.

Internos: Dentro de este tipo hay dos subtipos, por un lado tenemos empleados descontentos, normalmente de trabajos relacionados con la tecnología. Suelen hacer uso de los privilegios que se les ha asignado como trabajadores y por otro lado tenemos a pequeños ladrones que se aprovechan de los permisos que se les ha asignado como empleados o consultores.

Criminales profesionales: son especialistas en espionaje corporativo. En ocasiones tienen acceso a equipos de estado.

Guerreros Cibernéticos: suelen estar bien financiados. Mezclan la actividad política con la actividad criminal. En muchas ocasiones son activistas cibernéticos.

Además de esta clasificación, en el mundo de Internet es comúnmente aceptada la siguiente clasificación:

Black Hat Hackers: normalmente motivados por la búsqueda de dinero, buscan puntos débiles para romper la seguridad.

White Hat Hackers: son los conocidos como hacker buenos, son los que basan todo en la ética. Buscan vulnerabilidades de los sistemas, pero no para hacer daño, buscar hacer más seguros los sistemas o simplemente reconocimiento.

Gray Hat Hackers: buscan las vulnerabilidades y aprovechan la información que consiguen para ofrecer sus servicios. Aunque buscan un beneficio económico no buscan hacer daño como los Black hat.

Crackers: podrían ser una división de los black hat, entran en sistemas para robar información o dejar algún malware o puerta trasera. También se conoce como crackers a los que diseñan software para romper la seguridad de otros software.

Script Kiddies: son hackers novatos, se dedican a utilizar software creado por otros para penetrar en sistemas vulnerables. Desconocen el funcionamiento de software que utilizan.

Phreaker: es el hacker que comete sus delitos sobre sistemas telefónicos, ya sean tradicionales, móviles o a través de Internet. Surgen buscando realizar llamadas gratuitas.

Newbie: es que comienza en el mundillo, simplemente juega con las herramientas y manuales que hay en páginas web. En el mundillo no se considera hacker.

Lammer: es una persona que posee información de cómo hackear pero sólo lo utiliza para amenazar. En el mundillo no se considera hacker.

Carder: se conoce con esta denominación a un tipo de hacker que hace uso de tarjetas de créditos ilegitimas. Ya sean robadas o incluso creadas por él.

Pirata de software: estos ciberdelincuentes que se dedican a la modificación se software legítimo para distribuirlo o usarlo de forma ilegítima.

En España el código penal tipifica como delito la venta o compra de software ilegal.

Además de estos individuos, en los últimos tiempos se viene hablando de un concepto que está cambiando la forma de ver los hackers, y en el que organizaciones de defensa están poniendo su punto de mira. Se trata de los conocidos como APT (Advanced Perssistent Threat).
APT: Se entiende por APT a individuos o grupos con la capacidad de persistencia y efectividad para comprometer la seguridad de los sistemas informáticos. Se puede considerar que este grupo de atacantes suponen la profesionalización de la que hablaremos en otros puntos de este documento. Al ser profesionales disponen de los recursos necesarios para realizar un ataque (humanos y técnicos). Muchas veces actúan bajo el paraguas de los estados, que financian este tipo de grupos en su propio beneficio.

2.5. Quién persigue la ciberdelincuencia

Al estar hablando de delitos, por supuesto, son los propios cuerpos de seguridad de los distintos estados los que se encargan de perseguir la ciberdelincuencia, pero al tratarse de delitos en muchos casos específicos hay asociaciones y organismos que se han creado exprofeso o que se han especializado como el caso de INTERPOL.

A continuación vemos los organismos más importantes, directa o indirectamente en la lucha contra la ciberdelincuencia, no sólo a través de trabajo policial, sino también a través de normativas, convenios y formación que ayudan en la lucha contra la ciberdelincuencia.

INTERPOL: cómo no podía ser de otra forma son y han sido la referencia en la persecución del cibercrimen. En 2014 se abrirá el Complejo Mundial de INTERPOL para la Innovación en Singapur. Este centro pretende ser un centro puntero en la investigación y desarrollo de nuevas tecnologías para la detección de delitos y la identificación de delincuentes.

Ellos mismos definen como componente principal de este complejo mundial la seguridad digital, que incluye: (14)

(14) **Interpol.** Interpol. *El Complejo Mundial de INTERPOL para la Innovación.* [En línea] 2014 http://www.interpol.int/es/Acerca-de-INTERPOL/El-Complejo-Mundial-de-INTERPOL-para-la-Innovaci%C3%B3n.

- Un laboratorio forense encargado de prestar apoyo a las investigaciones sobre delincuencia digital;
- Investigación destinada a probar protocolos, herramientas y servicios, y a analizar las tendencias de los ciberataques;
- Elaboración de soluciones prácticas en colaboración con la policía, los laboratorios de investigación, el mundo académico y los sectores público y privado;
- Estudio de cuestiones tales como la gobernanza de la seguridad de Internet.

En definitiva afirma que la innovación es imprescindible para adelantarse a los delitos.

Interpol tiene una red de contacto siempre disponible, conocida como I-24/7 para la comunicación de los cuerpos policiales de todo el mundo. Dentro de esta red Interpol ha elaborado una lista de puntos de referencia nacionales (NCRP[9]) que cuenta actualmente con 121 puntos en todo el mundo.

Europol: la policía europea, que tiene como misión principal ayudar a las policías locales de los países miembros en la lucha contra de terminados delitos como terrorismo, tráfico de drogas o trata de seres de humanos, entre los delitos de los que la policía europea se encarga son los delitos cometidos a través de Internet.

En su propio documento de creación se prevé específicamente: “tareas de recogida y análisis de información en Internet para contribuir a identificar las actividades delictivas facilitadas por Internet o cometidas a través de Internet”. (15)

Europol colabora con los servicios policiales de los estados miembros de la Unión Europea, Australia, Canadá, Estados Unidos y Noruega.

Europol dispone de un sistema informático diseñado para el intercambio y análisis de información criminal en los países con los que colabora.

(15) **Europa, Consejo de.** *Decision 2009/371/JAI.*

[9] National Central Reference Points.

En junio de 2014 ENISA[10] (European Union Agency for Network and Information Security) y Europol firman un acuerdo estratégico de cooperación (16) en la Lucha contra la ciberdelincuencia. Esta cooperación consistirá en:

- El intercambio de conocimientos y competencias específicos
- La elaboración de informes situacionales generales
- Informes resultantes de análisis estratégicos y mejores prácticas
- El refuerzo del desarrollo de capacidades a través de la formación y la sensibilización, con el fin de salvaguardar la seguridad de la red y la información a nivel europeo.

Además de las redes de cooperación judicial es necesario compartir información, para ello hay multitud de herramientas como hemos comprobado, pero cabe destacar las bases de datos de Europol conocidas como AWF (Ficheros de trabajo de Europol): TWINS (Pornografía infantil, incluye información sobre víctimas y agresores, se utiliza para la búsqueda de información para la identificación y búsqueda de los agresores), MARITZA (Trata de Seres Humanos), COLA (Tráfico de drogas de organizaciones criminales latinoamericanas), MUSTARD (Tráfico de cocaína), SUSTRANS (Transacciones de dinero sospechosas) y TERMINAL (usa para la lucha contra las estafas electrónicas, especialmente el robo y duplicado de tarjetas de crédito en la red).

Consejo de Europa: El consejo de Europa tiene una Red de contacto 24/7, en la que están todos los países que forman parte de las convenciones sobre sobre cooperación en materia penal. El artículo 35 del Convenio Sobre Ciberdelincuencia del Consejo de Europa está dedicado a esta Red de contacto: (3)

> *"Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a*

(16) **Europol, ENISA y.** Comisión Europea. *Lucha contra la cibedelincuencia: ENISA y Europol firman un acuerdo estratégico de cooperación.* [En línea] 2014. http://ec.europa.eu/spain/pdf/ip270614%282%29.pdf.

(3) **Europa, Consejo de.** Convenio Europeo de Ciberdelincuencia. Budapest : s.n., 2001.

[10] ENISA tiene como objeto ayudar a los estados miembros de la UE, a la Comisión y a todas las partes implicadas en la prevención y la lucha contra problemas de seguridad de las redes y de la información.

sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a el asesoramiento técnico;

b la conservación de datos en aplicación de los artículos 29 y 30;

c la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

2 a El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.

b Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

3 Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red."

ONU: A través de su Asamblea general, en el año 2000 adopta la resolución 55/63 (17) que incluye: "Los Estados deben velar para que en su legislación y en la práctica se eliminen los refugios seguros para quienes utilicen la tecnología de la información con fines delictivos". Esta resolución viene a completar la 45/121 de 1990 sobre Prevención del Delito y Tratamiento del Delincuente. En 2010 adopta la Resolución 65/230, basada en el artículo 42 de la Declaración de El Salvador: *"Invitamos a la comisión sobre Prevención del Delito y Justicia Penal que considere convocar a un grupo intergubernamental de expertos de composición abierta para llevar a cabo un estudio exhaustivo del problema de la delincuencia cibernética y respuestas a la misma por parte de los Estados miembros, la comunidad internacional y el sector privado, incluido el intercambio de información sobre legislación nacional, las mejores prácticas, asistencia técnica y la cooperación internacional, con el fin de examinar opciones para intensificar las existentes y proponer nuevas respuestas jurídicas nacionales e internacionales a la ciberdelincuencia o de otro tipo de respuestas."*

(17) **Asamblea general de la ONU.** Resolución 55/63. [En línea] http://www.unodc.org/pdf/crime/a_res_55/res5563s.pdf.

A raíz de esta Resolución se crea el citado grupo internacional, organizado por la UNODC. En 2013 se presenta un borrador a discusión con las recomendaciones y la comisión decide los pasos siguiente. Actualmente continúan trabajando.

G8: desde 1997 tienen un subcomité sobre delitos de "alta tecnología". En la reunión del G8, celebrada EEUU los Ministros de Justicia e Interior adoptaron diez principios básicos, cuya meta era que ningún delincuente tenga refugio en cualquier lugar del mundo. En 2004 en una reunión similar que tuvo lugar de nuevo en Washington DC se emite el siguiente comunicado conjunto:

"Continuando el fortalecimiento las disposiciones jurídicas internas. Para construir capacidades globales para combatir usos terroristas y criminales de Internet, todos los países deben seguir para mejorar las leyes que tipifican como delito el mal uso de las redes informáticas y que permitirá la cooperación más rápido en las investigaciones relacionadas con Internet. Con el Convenio del Consejo de Europa sobre la ciberdelincuencia que entra en vigor el 1 de julio de 2004, debemos tomar medidas para fomentar la adopción de las normas jurídicas que contiene sobre una base amplia". En la reunión de 2005 se hizo hincapié añadiendo: *"Para garantizar que los organismos encargados de hacer cumplir la ley pueden responder rápidamente a las graves amenazas cibernéticas e incidentes".* En la reunión de Moscú de 2006 de nuevo se refieren a la ciberdelincuencia:
"También hablamos sobre temas relacionados con la compartición acumulado experiencia internacional en la lucha contra el terrorismo, así como el análisis comparativo de la legislación a ese respecto. Hablamos de la necesidad de fortalecer las medidas eficaces que prevendrán terrorismo electrónico y los actos terroristas en este ámbito de las altas tecnologías. Para ello es necesario disponer de un conjunto de medidas para prevenir esos actos criminales posibles, incluidos en el ámbito de las telecomunicaciones. Eso incluye el trabajo en contra de la venta de datos privados, información falsificada y la aplicación de los virus y otros programas informáticos dañinos. Vamos a instruir a nuestros expertos para generar enfoques unificados a la lucha contra la delincuencia cibernética, y vamos a necesitar una base jurídica internacional para este trabajo en particular, y vamos a aplicar todo eso para evitar que los terroristas utilicen sitios de computación e Internet para la contratación de nuevos terroristas y el reclutamiento de otros actores ilegales". En 2008 se presenta un informe sobre terrorismo internacional. En la reunión de Roma de 2009 afirmaron: *"El mal uso de lo Penal de redes sociales, servicios de cifrado, los servicios de VoIP, el sistema de nombres de dominio, y otros ataques criminales nuevas y en evolución en los sistemas de información, plantean desafíos a*

la aplicación de la ley aumentaron y se están extendiendo." En la reunión de 2011 en Deauville ya se incluía una sección sobre Internet.

Todo esto nos demuestra la preocupación del G8 sobre la ciberdelincuencia, haciendo hincapié en la importancia de tener unas leyes comunes en la lucha contra la ciberdelincuencia y en evitar la existencia de refugios para los ciberdelincuentes.

Para la persecución del cibercrimen y la coordinación de los estados contra este, el G8 ha creado una red internacional de contactos disponibles las veinticuatro horas del día, siete días a la semana, esta red exige a los países participantes[11] tener coordinadores para investigaciones transnacionales siempre disponibles.

OCDE: la Organización para la Cooperación del Desarrollo Económico está buscando una alianza de todos los actores involucrados en el cibercrimen: gobiernos, entidades de seguridad, proveedores de Internet, empresas y organismos de la sociedad civil.

La OCDE tiene un Grupo de Trabajo sobre Seguridad de la Información y Privacidad (WPISP) que tiene como mandato desarrollar unas políticas de análisis público y unas recomendaciones de alto nivel. Este Grupo de Trabajo mantiene una red activa de expertos del gobierno, industria y sociedad civil. En 1992 creó las Directrices sobre seguridad que se adoptó como Recomendación del Consejo de la OCDE de 25 de julio de 2002.

La OCDE se considera una de las organizaciones que más ha luchado contra el correo no deseado, en 2004 creó una Comisión Especial en contra del SPAM. Conocida como OECD Anti-spam Task Force que en 2006 estableció una serie de recomendaciones y políticas para combatir el SPAM a nivel internacional.

En 2008 en la reunión Ministerial de Seul, los países miembros acordaron *la Declaración Ministerial de la OCDE de Seúl sobre el Futuro de la Economía Internet* (18) una serie de premisas bajo el epígrafe de endurecer la ser confianza y seguridad a través de políticas que:

- Protejan información crítica de infraestructuras nacionales o internacionales contra riesgos de seguridad.

(18) **OECD, Ministerial session.** OECD.org. *The Seoul Declaration for The Future of the Internet Economy.* [En línea] 2008. http://www.oecd.org/internet/consumer/40839436.pdf.

[11] Actualmente esta red está conformada por 58 países.

- Fortalecer la resistencia y la seguridad de Internet y lo relacionado con redes de dispositivos y sistemas TIC para aumentar las demandas y necesidades de nuestras economías y sociedades.

- Reducir la actividad maliciosa online a través de refuerzos nacionales e internacionales de la cooperación de comunidades de interesados encaminadas a la prevención, protección, intercambio de información, respuesta continuidad de negocio y recuperación

- Asegurar la protección de las identidades digitales y los datos personales y la privacidad de los individuos en línea.

- Fomentar la colaboración entre los gobiernos, el sector privado, la sociedad civil y la comunidad técnica de Internet para que construyan un informe sobre el impacto de Internet en los menores con el fin de mejorar su protección y apoyo.

- Promover la investigación sobre las nuevas amenazas de seguridad.

- Apoyar la expansión del acceso a Internet y lo relativo a las TIC, especialmente para las personas en países en desarrollo.

- Facilitar la introducción de nombres de dominio internacionalizados IDNs mientras aseguran la integridad y estabilidad de Internet.

- Incrementar la cooperación de los gobiernos y las autoridades en las áreas de mejora en ciberseguridad, combatiendo el SPAM, así como protegiendo la privacidad, los consumidores y los menores.

Además la OCDE ha presentado varios informes sobre malware, e identidad online.

Foro de Cooperación Económica Asia-Pacífico (APEC): el Foro de Cooperación Económica Asia-Pacífico es un organismo creado para fortalecer el crecimiento económico y fomentar el comercio y las inversiones del bloque de la cuenta del pacífico, en este organismo participan los gobiernos de los siguientes países: Australia, Brunéi, Canadá, Indonesia, Japón, Corea del Sur, Malasia, Nueva Zelanda, Filipinas, Singapur, Tailandia, Estados Unidos, China Taipéi, China, México, Papús Nueva Guinea, Chile, Perú, Rusia y Vietnam. APEC tiene un Grupo de Trabajo sobre Telecomunicaciones e Información (APEC-TEL) cuyo propósito es mejorar las telecomunicaciones e infraestructura de la información de la región Asia-Pacífico, además dentro del grupo hay un subgrupo sobre Seguridad y Prosperidad que tiene el mandato de la

promoción de la seguridad y la confianza en el uso de las redes y sistemas, la creación de un equipo de respuesta a emergencias de cómputo (CERT) y un equipo de respuesta a incidentes de seguridad informática (CSIRT), así como la prevención del SPAM y el spyware y la capacitación en la lucha contra la ciberdelincuencia de los países miembros.

En 2002 el APEC lanza una estrategia en materia de seguridad que insta a los países miembros a adoptar medidas y a adoptar la legislación tomando como referencia el convenio sobre ciberdelincuencia de la Comisión Europea.

En la reunión de 2008 llegan al acuerdo de tomar medidas para estrechar la colaboración transfronteriza entre los miembros del APEC.

El Grupo de Trabajo APEC-TEL organiza gran número de formaciones para implementar la resolución de Naciones Unidas 55/63.

Commonwealth: las naciones que pertenecen a la Commonwealth[12] crearon en 2002 una ley modelo llamada Acta de Delitos relacionados con Sistemas de Cómputo (Computer Related Crimes Act). Esta ley de nuevo toma como referencia el Convenio sobre Ciberdelincuencia del Consejo de Europa y ha sido utilizada por varios de los países en la elaboración de leyes.

Organización de estados americanos (OEA): La Organización de Estados Americanos es un organismo formado por 35 países del continente Americano. La OEA se encarga de cuestiones de ciberdelito y terrorismo bajo el mandato de la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA).

En 1999 se crea el Grupo de Expertos Gubernamentales sobre Delito Cibernético que tiene el mandato de "fortalecer la cooperación internacional en la investigación y persecución del delito cibernético, facilitar el intercambio de información y de experiencias entre sus integrantes y formular las recomendaciones que sean necesarias para mejorar para mejorar y fortalecer la cooperación entre los Estados miembros de la OEA y con otras organizaciones o mecanismos." (19)

(19) **OAE.** Portal Interamericano de Cooperación en materia de Delito Cibernético. [En línea] http://www.oas.org/juridico/spanish/cybersp.htm.

[12] Los países miembros de la Commonwealth se pueden consultar en: http://thecommonwealth.org/member-countries

Como hemos visto los diferentes organismos buscan la forma de solicitar datos entre países. Hay grandes alianzas que corresponden con las alianzas clásicas a niveles económicos. Las redes 24/7 se han convertido en un gran instrumento, pero no es el único:

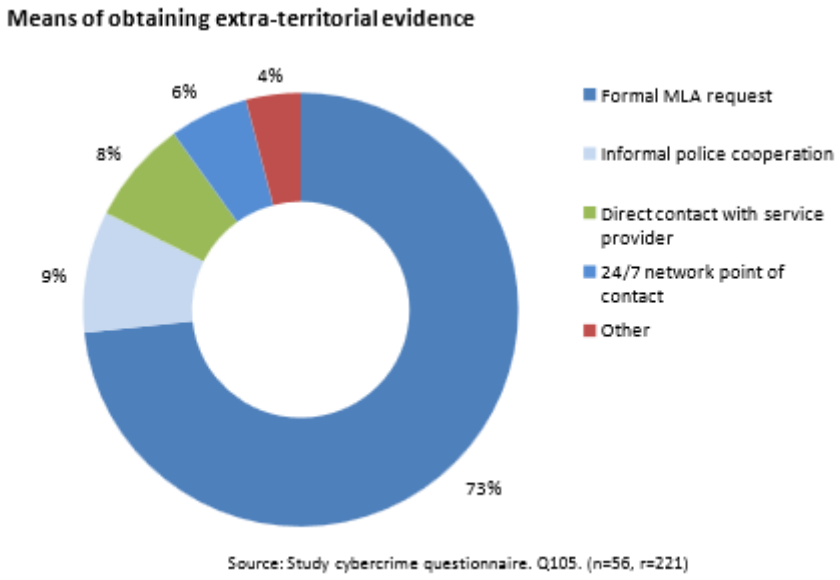

Figura 4. Formas de colaboración para obtener evidencias entre países. Fuente: ONUDC (7)

Como vemos en el gráfico, hay peticiones **formales MLA** (Mutual Legal Assistance Request) que son peticiones específicas de un país a otro, normalmente de evidencias en un caso criminal. Hablamos de asistencia mutua porque aunque se produce en un sentido, las peticiones pueden producirse en cualquier momento. Normalmente son peticiones entre mismo niveles de ambos países, normalmente policía a policía, este tipo de peticiones son las más comunes. También hay **peticiones informales** policía a policía. Peticiones directas a los proveedores de servicio. Las redes 24/7 también se han convertido en un gran medio para las peticiones, pero todavía suponen un escaso 6%.

La prevención del crimen comprende estrategias y medidas que buscan reducir los riesgos de que ocurra un cibercrimen, además de reducir los efectos en la sociedad y en las personas. En el informe de la ONUDC (7), solo el 40% de los países que contestaron a las preguntas del informe aseguraron tener una ley nacional o política contra el cibercrimen. El 20% tiene iniciativas en preparación.

(7) **United Nations Office on Drugs and Crime.** *Comprehensive Study on Cybercrime.* Viena : s.n., 2013. UNODC CCPCJ EG.4.

Organización del Tratado del Atlántico Norte (OTAN): aunque la alianza integró la seguridad de los sistemas TIC en la agenda de la Cumbre de Praga de 2002, no es hasta la cumbre de Lisboa de 2010 cuando establece que los ciberataques constituyen una de las nueva amenazas de las que se debe hacer cargo. En esta cumbre se propone desarrollar capacidades específicas para garantizar la defensa del ciberespacio, así como la integración en los planes de defensa de la alianza de la ciberdefensa.

En junio de 2011 los ministros de defensa de la alianza aprueban la nueva política de la OTAN en materia de ciberdefensa que sería integrada en la cumbre de Chicago de 2012 en la iniciativa defensa inteligente para el desarrollo conjunto de cibercapacidades.

Organizativamente la OTAN dispone del "Cyber Dfence Managment Board" en que se encuentran responsables políticos, militares, operativos y técnicos con responsabilidades en materia de ciberdefensa. Este organismo tiene como misión la coordinación de las actividades de ciberdefensa del cuartel general de la ONU y los comandos y organismos asociados.

En el plano operativo en 2012 se crea la Agencia de Comunicación e Información de la OTAN (NCIA[13]) que tiene como objetivo la provisión de ciberseguridad a las capacidades de la OTAN. En 2014 se revisaron los objetivos y NCIA reorganizó sus servicios dejando su misión en cuatro áreas: ciberdefensa, Garantizar la Información, Seguridad de la Información y Seguridad CIS.

La NCIA proporciona a la alianza servicios técnicos y operativos en materia de ciberdefensa y ciberseguridad. Estos servicios los ofrece a través del NCIRC (NATO Computer Information Response Capability). Este programa se inició en 2012 y a finales de 2013 se consideró completamente operativo, con capacidades de última generación, tras una inversión de cerca de 60 millones de euros.

En marzo de 2013 comienza el proyecto Multinational Cyber Defence Capability Development de la mano de NCIA, con este proyecto creado por Canadá, Países Bajos, Dinamarca, Noruega y Rumania se quiere mejorar la cooperación en materia de ciberseguridad mediante la financiación conjunta de proyectos de I+D+i. Actualmente están trabajando en tres líneas, la compartición de información, el estado de ciber-situación y tecnologías DMCCI[14].

[13] NATO Communications and Information Agency
[14] Distributed Multi-sensor Collection and Correlation Infraestructure. Es un proyecto que busca mejorar la habilidad para encontrar actividad maliciosa de APT (Advanced Perssistent Threat). Se entiende por APT a individuos o grupos con la capacidad de persistencia y efectividad para comprometer la seguridad de los sistemas informáticos. Ver punto 2.4 de este documento

Para apoyar a la industria se ha creado el Grupo Asesor Industrial de la OTAN (NIAG), este grupo busca apoyar en la creación de consorcios en materias de ciberseguridad. En estos momentos están analizando la posibilidad de una alianza en caso de ataque cibernético.

Para la formación en materia de ciberdefensa, ha desarrollado el Centro de Excelencia de Ciberdefensa de Tallín. Es una organización militar al servicio de la OTAN con la misión de mejorar la capacidad, cooperación y compartición de información a lo largo de la OTAN a través de la educación y la investigación. En agosto de 2014 ha organizado el curso de sobre Leyes Internacionales de ciberoperaciones con la presencia de 26 países. Cada año celebra la conferencia internacional sobre ciberconflictos, conocida como CyCon, la de 2014 tuvo su foco en la defensa activa, la de 2015 lo tendrá en la construcción de Internet y su futuro desarrollo.

En la actualidad se están cerrando acuerdos con la Unión Europea para colaborar en materia de ciberdefensa, acuerdos similares a los que ya existen con Austria, Finlandia, Irlanda, Suecia y Suiza.

En junio de 2014 los ministros de defensa de la OTAN aprobaron la nueva política de defensa cibernética, que se está aplicando en la actualizad, “La nueva política y su aplicación se mantendrán bajo estrecha, tanto a nivel político como técnico dentro de la Alianza y se perfeccionarán y se actualizan de acuerdo con la evolución de la amenaza cibernética.” (20)

Unión Europea: se considera que el comienzo de la política Europea sobre ciberdelincuencia comienza la Comunicación conjunta del Consejo y de la Comisión de 2000 (COM/2000/890). En 2002 se trabaja en una directiva marco para la lucha contra ciberataques y la armonización del derecho penal y la persecución penal (COM/2002/173) que entraría en vigor al año siguiente. Al ser una directiva vinculante los estados tienen la obligación de transponerla a su jurisdicción en el plazo de un año.

En 2012 se aprueba la Estrategia de seguridad en equipos informáticos (COM/2012/529) que regula la seguridad y la fiabilidad de los centros de datos europeos. En febrero de 2014 el Parlamento Europa aprueba la Directiva sobre Seguridad de la Información y Redes (NIS) (COM/2013/48) destinada a las empresas y que obliga a las empresas a cumplir los estándares de seguridad. También obliga a las empresas a informar de los ciberataques significativos a través de los centros de alerta nacionales.

(20) **OTAN.** NATO and cyber defence. [En línea] 2014. http://www.nato.int/cps/en/natolive/topics_78170.htm.

La unión Europea publicó en 2013 a través de la Comisión Europea y junto con la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad la **Estrategia de Seguridad** (21), además presentó una propuesta de directiva de la Comisión sobre la seguridad de las redes y de la información (SRI). La estrategia define 5 prioridades: (22)

- La ciberresiliencia.
- La reducción drástica de la delincuencia en la red.
- El desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD).
- El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad.
- El establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

La directiva unifica también las políticas de funcionamiento de los conocidos como CERT. Tanto el CERT-EU como los CERT de los distintos países.

Los CERT[15] son los Equipos de Respuesta ante Emergencias Informáticas, se trata de un grupo de expertos que desarrollan medidas preventivas y reactivas sobre ataques relacionados con ataques informáticos.

2.6. Costes de la ciberdelincuencia

El informe de junio de 2014 del CSIS[16] sobre el impacto económico del coste del cibercrimen (23) estima que el coste anual del cibercrimen en todo el mundo es superior a 400.000 millones de dólares. En este coste se estima lo que ha afectado a personas, entidades y países.

Cientos de millones de personas ven como sus datos personales son robados, sólo en EEUU 40 millones de personas se han visto envueltas en un incidente de este tipo. A continuación vemos los cinco países con mayor número de personas afectadas según el informe del CSIS.

(21) **Comisión Europea.** *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Comisión Europea.

(22) **Wegener, Henning.** *LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA.* 2014.

[15] CERT – Computer Emergency Response Team
[16] Center for Strategic and International Studies.

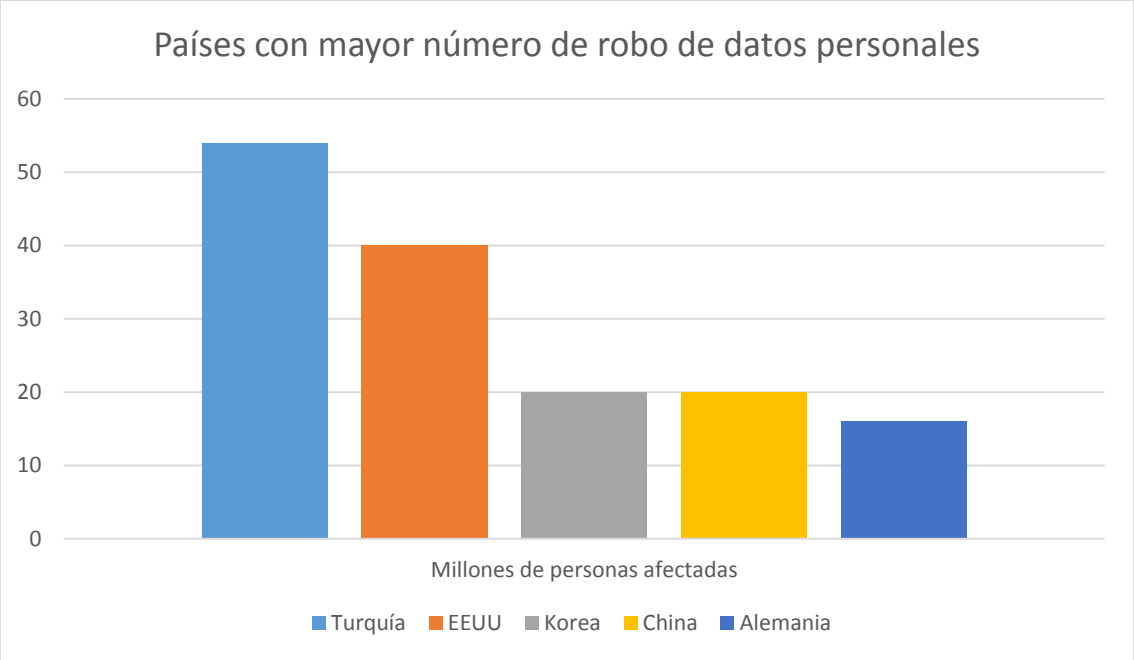

Figura 5. Países con mayor número de robo de datos personales. (23)

Aunque este tipo de robos no son fáciles de convertir en dinero, el impacto en la opinión pública es muy grande y genera inseguridad y falta de confianza. Puede hacer ver a la opinión pública que el cibercrimen está fuera de control. Este tipo de delito puede afectar al empleo, se estima que en Europa se pueden perder 150.000 trabajos debido al cibercrimen.

Aunque el coste económico es importante, la ciberdelincuencia tiene otra serie de costes, que a su vez tendrán un impacto económico. La ciberdelincuencia puede afectar a las compañías de muchas formas, desde el rendimiento de la empresa, a la imagen de marca, la innovación o produciendo una pérdida de competitividad. Este tipo de daño se va incrementando a medida que las transacciones y posición en Internet son cada vez más importante.

Las pérdidas de propiedad intelectual hace que las empresas y países pierdan capacidad competitiva y en muchos casos hace que terceros se aprovechen de la investigación y desarrollo de terceros. Pero el coste estimado de los robos de propiedad intelectual es prácticamente imposible de calcular como otros intangibles.

Uno de los problemas a la hora de ver los costes de la ciberdelincuencia es que la mayoría de los países no tienen datos concretos. Si vemos sólo los casos conocidos y documentados, en EEUU por ejemplo, el gobierno habla de más de 3.000 empresas víctimas de un ataque en el

(23) **Center for Strategic and International Studies.** *Net Losses: Estimating the Global Cost of Cybercrime.* Washington, DC : s.n., 2014.

año 2013. En el ataque a dos bancos en Golfo Pérsico se perdieron 45 millones de dólares en unas horas. Muchos de los ciberataques son ocultados o no se sabe el alcance del ataque. Cuando Google fue atacado en 2010 muchas compañías fueron afectadas, pero sólo lo sabemos porque lo sacó a la luz pública Wikileaks.

Uno de los ciberdelitos que más está creciendo es la manipulación de los mercados bursátiles mediante la obtención de información privilegiada, este tipo de delito es muy difícil de detectar, perseguir y cuantificar.

A todos estos costes hay que añadir el gasto en seguridad y lo que cuesta recuperarse de un ciberataque.

Hay un gasto que en ocasiones no se tiene en cuenta, el del tiempo perdido por culpa del cibercrimen, Norton en su informe 2011 (6) estima que el coste del tiempo traducido en dólares es de 274.000 millones de dólares. El porcentaje de adultos que han sido víctimas de un cibercrimen es alarmante:

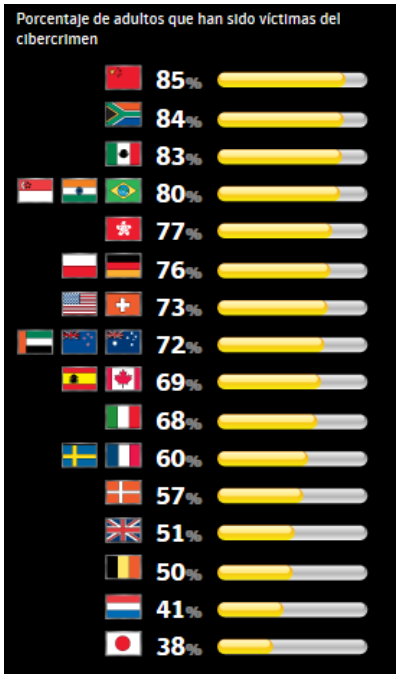

Figura 6. Puntos calientes de los ataques. Norton (6)

(6) **Norton Symantec.** *Informe sobre el cibercrimen Norton.* 2011.

El coste de la ciberdelincuencia en función del producto interior bruto nos permite ver la importancia que esta tiene:

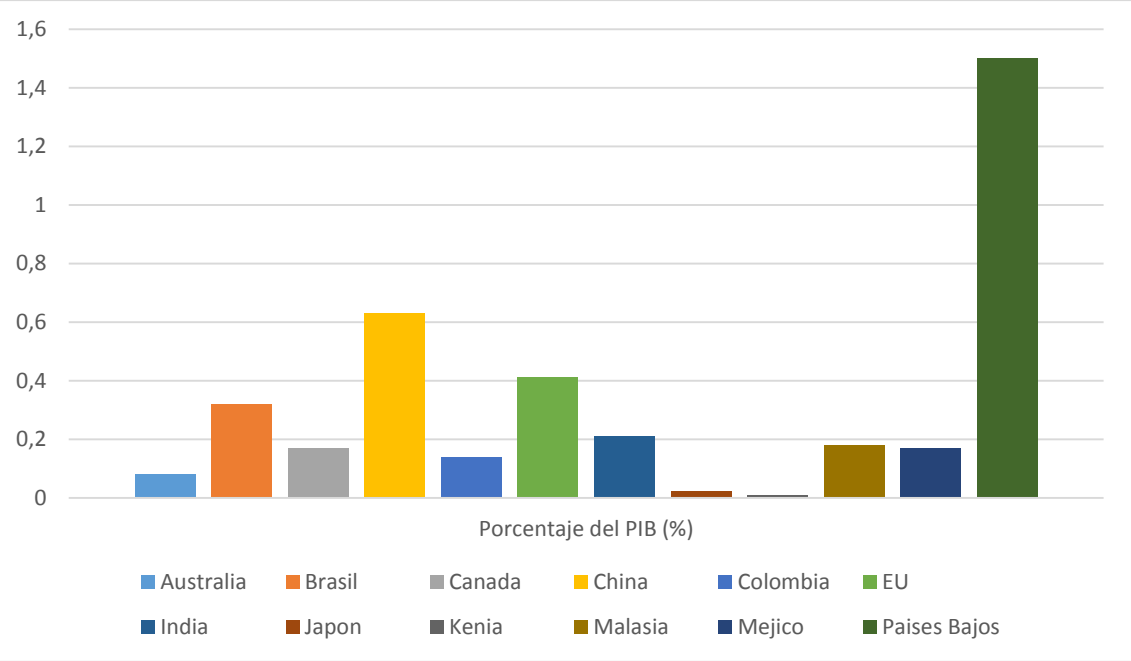

Figura 7. Porcentaje del Producto Interior Bruto. (23)

Como vemos aunque parecen cantidades bajas, estamos hablando de una cantidad lo suficientemente importante en todos los países.

2.7. Futuro de la ciberdelincuencia

La ciberdelincuencia es cada vez un negocio más lucrativo, por lo que sólo podemos esperar que cualquier delito que reporte dinero al atacante siga aumentando, uno de los delitos que más se espera que aumente es el robo de datos, ya sea de datos empresariales, gubernamentales o privados. También aumentarán las técnicas de evasión de impuestos.

A nivel de ataque contra el usuario de a pie, parece claro que la tendencia moverá los ataques de plataforma, actualmente la plataforma más atacada es Windows, pero cada vez se venden menos equipos considerados PC (ya sean sobremesa o portátil), y cada vez se venden más equipos móviles, por lo tanto parece seguro que los ataques cada vez más irán dirigidos a los dispositivos móviles, cualquiera que sea el sistemas operativo, pero siempre apuntando a los mayoritarios, ahora mismo Android e IOS.

(23) **Center for Strategic and International Studies.** *Net Losses: Estimating the Global Cost of Cybercrime.* Washington, DC : s.n., 2014.

Además de esto, el movimiento de datos hacia la nube hace que estos sistemas vayan a ser también objeto de ataques.

La automatización de los sistemas de acceso y uso de sistemas públicos, por ejemplo al transporte público también va a ser uno de los puntos de batalla en los próximos años. Ya se han visto caso de casos de ataque por ejemplo en sistema de alquiler de bicicletas del ayuntamiento de Madrid.

También veremos un aumento de las botnets y de los equipos zombies, que como ya hemos comentado es posible que pasen de los PC a los dispositivos móviles.

Cada día más nos enfrentamos y nos enfrentaremos a una profesionalización del cibercrimen, llegando incluso a la creación de proveedores de servicios criminales.

Los proveedores de servicios cada vez tienen más datos nuestros, servicios como google now saben cuándo estás en el trabajo o en casa, cuando vas en coche o donde has aparcado, lo que hace cada vez más importante la seguridad de estos sistemas. Cada vez más nos vamos a encontrar con que problemas de seguridad de un servicio afectan a la seguridad de las personas.

Al igual que los ciberdelitos y el cibercrimen avanzan, también avanzan los medios de lucha y sobre todo la unión de los países para la lucha, en los próximos años veremos cada vez más alianzas en la lucha contra el cibercrimen y sobre todo en mecanismos de defensa. Las alianzas I+D+i serán las que hagan avanzar a los estados en esta materia.

CAPÍTULO 3.
JURISDISCIÓN EN MATERIA DE CIBERDELINCUENCIA

3. Jurisdicción en materia de ciberdelincuencia

Internet, cibercrimen, ciberdelito, suenan a conceptos de moda, pero el cibercrimen no es un concepto nuevo, ya en 1976 Francia encarga un informe en el que se ve la preocupación del gobierno galo sobre el cambio de paradigma que Internet iba a producir, en este informe finalizado el año siguiente Simon Nora acuña el concepto telemática (24) y anticipa como la técnica constituye un factor de aceleración en todos los ámbitos de la sociedad.

También en 1977 el gobierno de EEUU elabora un estudio sobre la problemática asociada a los programas de computadora. En 1979 Interpol impartía la primera conferencia internacional sobre ciberdelincuencia.

En 1982 la OCDE convoca un grupo de expertos en derecho para crear una legislación penal para la protección de programas y sistemas informáticos, a raíz de este grupo surge el informe "*Computer Related Crime: Analysis of the Legal Policy*" que establece propuestas para la modificación de los códigos penales de distintos países.

En 1989 el Consejo de Europa elabora unas directrices dirigidas a los parlamentos de los países miembros para que estos las incorporen a sus respectivas legislaciones. Para ello crea el *Comité especial de expertos sobre delitos relacionados con el empleo de la computadora.* La resolución que llega como conclusión de este comité insta a los estados miembros a tener en cuenta la delincuencia relacionada con las computadoras cuando revisen o preparen una nueva ley.

En 1990 la ONU añade a su agenda el tema de la delincuencia informática, afirmando que se facilita enormemente la realización de operaciones delictivas, esto será el preámbulo del *Manual de las Naciones Unidas sobre prevención y control de Delitos informáticos* de 1994.

Estos informes, estudios y directrices son los antecedentes a lo que será el documento de referencia en materia de ciberdelincuencia: El *Convenio sobre Ciberdelincuencia* del Consejo de Europa.

A niveles nacionales se ha intentado adecuar las leyes a los nuevos delitos, como es lógico unos países lo han hecho mejor y otros peor, pero todos comparten la misma problemática. Con la llegada de Internet llegan nuevos delitos como la intrusión en redes informáticas que

(24) **Nora, Simon y Min, Alain.** *La informatización de la sociedad.* 1977.

poco a poco se van introduciendo en las legislaciones, el problema es que estos procesos son lentos y en muchas ocasiones la ciberdelincuencia va muy por delante de los estados. En otros casos los delitos son similares a los que se pueden producir fuera de la red, lo que supone una facilidad a la hora de adecuar las leyes.

Se considera que hay tres etapas a la hora de ajustar las leyes nacionales, se debe empezar por el reconocimiento de la utilización delictiva de la red, la segunda etapa sería identificar las lagunas que puedan existir en el código penal y la tercera etapa es la redacción de la nueva legislación, este proceso es complejo y surge un problema en la redacción de este tipo de leyes si no hay una cooperación internacional. Por eso es imprescindible la existencia de convenios como el convenio de Budapest.

3.1. Problemática de las leyes en Internet

Internet y sus características, principalmente el principio de neutralidad que básicamente da libertad al usuario para moverse por Internet sin fronteras, hacen que legislar en este ámbito se convierta casi en una quimera, los tratados y convenios entre países parecen el único paso lógico para conseguir que los delitos sean perseguidos y que las penas y consecuencias no dependan de otras cosas. Aunque esto suena idílico es prácticamente imposible cuando lo que se persigue no es delito en todos los países.

Otra de las características que influyen en esta problemática es transnacionalización de Internet y una de sus características principales, la descentralización. Este carácter distribuido, la forma de malla que caracteriza la red hace que, a priori, nadie pueda decidir que conecta con qué. En Internet no existe una entidad central que controle la información que circula o sea capaz de establecer unas normas aceptadas por todos los países.

Más allá de la problemática de perseguir un determinado delito, este carácter transnacional genera tensiones entre países con espacios jurídicos diferentes. Otro de las grandes problemáticas a la hora de legislar es el anonimato en la red, aunque cada vez es más fácil saber la dirección de origen (IP) desde la que se produce un delito, no es nada sencillo saber quién está detrás de esa dirección. Además, como veremos en el apartado dedicado a redes oscuras de este mismo documento, es relativamente fácil acceder a la red de forma anónima. Este anonimato genera en muchos casos tensiones, ya que en muchas ocasiones lo único que se conoce es el origen de un ataque, y, se extrapola el ataque a todo un país. Es muy sencillo ver titulares del tipo: “*activista de origen xxx ataca la web de...*”.

Los centros de datos donde se encuentran los servidores en muchos casos se encuentran en lugares que no son revelados por seguridad, en estos centros de datos pueden convivir desde la información de un banco a la información de un ciberdelincuente, por ejemplo una difamación sobre una persona es muy difícil de eliminar si no sabemos dónde está albergada la web en la que ha sido publicada. Esta situación de ubicuidad puede dar situaciones curiosas, en las que un delincuente se encuentre en un país, la víctima en otro, y los datos que han generado la situación en un tercer país. Esto hará que la persecución del delito sea muy compleja y necesite de la colaboración entre los distintos estados.

La forma de realizar los delitos, la capacidad de hacerlo a distancia y la complejidad de conseguir información sobre el ciberdelincuente hacen que el intercambio de información antes y después de la comisión del delito, una vez se ha detenido al delincuente y durante el enjuiciamiento sea de vital importancia, como hemos visto anteriormente, los estados empiezan a tomar medidas en este sentido, como el uso de las redes 24/7.

Otro de los problemas a la hora de legislar en Internet, al igual que a la hora de perseguir a los ciberdelincuentes, es que en muchos casos estos van un paso por delante de las autoridades. Además modificar la legislación no es un proceso rápido en casi ningún país, lo que hace que los delitos específicos no tipificados como tal en la legislación "clásica" sean más complicados de perseguir.

Con el fin de mitigar estos problemas se han creado varias redes de cooperación judicial.

Eurojust: es un órgano de la Unión Europea encargado de la coordinación judicial de los estados miembros. Se crea en 2002[17] con el fin de reforzar la lucha contra el crimen transfronterizo, como hemos visto, esta es una de las principales características del cibercrimen. Está formado por un miembro de cada uno de los Estados miembros de la UE.

Iberred: en este caso es la Comunidad Hispanoamericana de Naciones quien crea en 2004 esta red con un fin similar al de Eurojust, en este caso optimizar la asistencia civil y penal y reforzar la cooperación entre los 23 países que componen la comunidad.

Entre esas dos redes hay un Memorandum de Entendimiento, que como se indica en el mismo *"El propósito de este Memorándum de Entendimiento es consolidad la relación entre Eurojust e*

[17] Se crea en la Decisión del Consejo 2002/187/JAI del 28 de febrero de 2002.

Iber-RED con la intención de reforzar la lucha contra las formas graves de delitos transnacionales." (25)

3.2. Análisis del Convenio Europeo sobre Ciberdelincuencia

La Unión Europea no establece normas penales ya que es una parcela que queda reservada a la soberanía de los Estados. La forma de obligar, o mejor dicho de obligarse que tienen los estados son los convenios, directivas y tratados, que en el momento que son firmados y ratificados obligan a los Estados a su cumplimiento.

A nivel europeo, la cooperación es un hecho, al menos en materia policial, el protocolo de Schengen, que además de acordar la supresión de las fronteras incorpora medidas para la cooperación policial y judicial y de armonización de legislaciones, y Europol así lo atestiguan.

La armonización normativa en delitos informáticos como hemos visto en el punto anterior es totalmente necesaria, en el ámbito procesa es complicadísimo elaborar tratados internacionales que impongan[18] normas a los Estados, a nivel europeo el consejo puede hacer uso de directivas para el funcionamiento del mercado común tal y como establece en su artículo 94[19]

El primer intento para realizar esta armonización en materia de ciberdelincuencia es el Convenio Europeo Sobre Ciberdelincuencia, también conocido como Convenio de Budapest.

EL Convenio fue redactado por el Consejo de Europa[20] en 2001 y en 2003 se le añadió un protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.

Ha sido firmado por los países miembros de la Unión Europea, Canadá, Japón, Estados Unidos y Sudáfrica, aunque está pendiente de la ratificación de un gran número de ellos, España lo ratificó el 3 de junio de 2010.

(25) **Eurojust e Iber-RED.** *Memorandum de Entendimiento entre Eurojust e Iber-RED.* Mayo 2009

[18] El principio jurídico *pacta sunt servanda* vincula a los estados parte de un tratado, aunque son los estados los que deben decidir la transposición de las normas a su legislación.

[19] El consejo adoptará por unanimidad, a propuesta de la Comisión y previa consulta al Parlamento europeo y al Comité Económico y Social, directivas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que incidan directamente en el establecimiento o funcionamiento del mercado común

[20] El Consejo de Europa no está ligado a la Unión Europea, es una organización regional internacional. Está formado por todos los países miembros de la UE menos Bielorrusia, Kazajistan y el Estado Vaticano. Participan como observadores Estados Unidos, Canadá, Japón, México y Santa Sede.

Los antecedentes del convenio datan de 1983, año en el que un grupo de expertos se reúne y recomienda a la Organización de para la Cooperación y desarrollo económico la armonización en el ámbito de los delitos informáticos y realiza un informe que será entregado tres años después. A raíz de este informe el Consejo de Europa comienza a trabajar en el tema y en 1989 publica la primera Recomendación. En 1997 comienzas las negociaciones para la creación del tratado, en la cumbre de Estrasburgo de 1997 se establece un Plan de Acción por parte de los Jefes de Estado y de Gobierno del Consejo de Europa, en busca una respuesta común ante los cambios y desarrollo de las tecnologías de la información y comunicación. En el año 2000, en la reunión de los Ministros de Justicia e Interior de la Unión Europea de Marsella se decide dejar al Consejo de Europa finalizar la elaboración del tratado, del que por aquel entonces existían hasta treinta versiones. El abril de 2000 se publica el Proyecto de Convención de sobre el Delito Cibernético que aprobaría el Comité de Ministros el 8 de noviembre de 2001.

El convenio consta de 48 artículos (los artículos 2 a 13 dedicados a Derecho Penal[21] Internacional y los artículos 14 a 35 a Derecho Procesal Internacional) y un preámbulo, está estructurado en cuatro capítulos, que se encuentran divididos en secciones y títulos:

- **Capítulo 1.** (Artículo 1) Está destinado a aclarar terminología utilizada en el resto del documento.

- **Capítulo 2**. (Artículos 2 al 22) Titulado "Medidas que deberán adoptarse a nivel nacional", incluye los tipos de delito y los elementos procesales que sugiere en cada caso, como responsabilidades, jurisdicción, daos, salvaguardas, etc.

- **Capítulo 3**. (Artículos 23 al 35) Dedicado a la cooperación Internacional. Afronta el problema de la compartición de información de los estados, las extradiciones, la asistencia mutua, etc. Habla de la creación de una red 24/7 de cooperación entre los firmantes del tratado.

- **Capítulo 4**. (Artículos 36 al 48) Incluye las clausulas finales típicas de cualquier documento de este tipo, desde la fecha de entrada en vigor a las condiciones para la adhesión. También incluye un artículo que indica que en caso de controversias será el Comité Europeo Para Problemas Criminales el organismo al que se deberá acudir.

Como vemos el convenio llama a la tipificación como delito de determinadas conductas buscando la armonización del Derecho de los estados, aunque el Convenio se considera un

[21] El derecho procesal trata sobre los procedimientos, mientras que el penal sobre los delitos.

referente, no está exento de críticas, uno de los puntos que más controversia genera es el que se refiere a la posesión de *"cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos"* (3) en el artículo 6 del Convenio, ya que la posesión de este tipo de herramientas no tienen por qué implicar la intención de cometer un acto delictivo.

El otro punto conflictivo es lo referente a la cooperación internacional y el fomento de la compartición de datos, este tipo de información en muchos casos de carácter personal[22] pueden suponer un problema de protección de datos, incluso el incumplimiento protección del derecho a la intimidad y confidencialidad de ciertos datos. Incluso en Grupo de Trabajo sobre Protección de Datos de la Unión Europea tildó la redacción del Convenio como "con frecuencia demasiado vaga y confusa". Aunque el artículo 28 se refiere a la confidencialidad y restricciones de uso. El citado grupo de trabajo señala que sería conveniente obligar a subscribirse al Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. El principal problema es que el convenio no habla de autorización judicial para la solicitud de este tipo de datos, la injerencia en los datos personales por parte de las autoridades estatales son una intromisión en las libertades personales. En casi todas las jurisdicciones este tipo de petición responde a una resolución judicial. Se debe tener especial cuidado en este sentido cuando se traslade el convenio a las diferentes legislaciones, ya que se pueden estar cometiendo delitos contra los Derechos Humanos en lo que respecta a intimidad y protección de datos.

En el Convenio se intenta unificar criterios relacionados con la jurisdicción, concretamente en el artículo 22 que forma parte del capítulo 2, en este sentido afirma que el Estado tendrá **jurisdicción** cuando:

- El delito se haya cometido en su territorio
- El delito se produzca en buque que enarbole su pabellón
- El delito se produzca a bordo de una aeronave matriculada según sus leyes

(3) **Europa, Consejo de.** Convenio Europeo de Ciberdelincuencia. Budapest : s.n., 2001.

(41) **Europa, Consejo de.** *Convenio 108.*

[22] Hablamos de datos personales cuando: "constituyen toda aquella información personal que pueda conducir a la identificación de un individuo. Puede tratarse del nombre, la dirección, el número de teléfono, los datos bancarios, los resultados de exámenes médicos, el expediente académico, las transacciones comerciales, la dirección de correo electrónico, etc." (41)

- El delito sea cometido por uno de sus nacionales, si el delito es objeto de sanción en el país en el que ha sido cometido o ningún Estado tiene competencia territorial frente al mismo

Cuando hablamos de jurisdicción, el siguiente término que debemos analizar por su estrecha relación es la extradición, que también contempla el Convenio en su artículo 24. Aunque remite al Convenio de Extradición y otros acuerdos existentes en la materia, especifica que serán objeto de extradición los delitos que estén contemplados en las dos partes implicadas siempre que la pena sea de, al menos, un año.

Uno de los problemas que surgen cuando se juzga un caso de ciberdelincuencia es la existencia de evidencias o pruebas, en gran medida porque pueden resultar fáciles de eliminar, por ello el Convenio habla de conservación rápida de los datos informáticos, que recalca son susceptibles de pérdida o modificación, entregándolos rápido a la autoridad competente. Habla también de peticiones de datos a particulares y proveedores de servicios en Internet y del registro y confiscación de datos. También se contempla la interceptación de las comunicaciones en el caso de delitos considerados graves.

El Convenio contempla la necesidad de proteger nuevos bienes jurídicos que no están supuestos en el derecho penal.

Como conclusión podemos decir que el Convenio buscar armonizar el derecho internacional, estableciendo medidas procesales adaptadas al ciberdelito y establecer medios de cooperación internacional rápidos.

Protocolo adicional:

En el Convenio se echan en falta los delitos de índole racista y xenófoba cometidos a través de Sistemas informáticos, por ello como ya hemos comentado el Consejo de Europa en 2003 aprueba el protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medios de sistemas informáticos.

Este documento al igual que el convenio se divide en cuatro capítulos:

- **Capítulo 1**. (Artículos 1 y 2). En él encontramos la finalidad del documento, que no es otra que completar el Convenio de Budapest y las definiciones que afectan al documento y no se encuentran en el Convenio de Budapest.

- **Capítulo 2**. (Artículos 3 al 7). En él se describen las medidas que se deben tomar a nivel nacional para la lucha contra la difusión, las amenazas, los insultos o la negación de crímenes contra la humanidad. También se tipifica como delito la cooperación y complicidad en este tipo de delito.

- **Capítulo 3**. (Artículo 8). Explica la relación entre el protocolo y el Convenio. En general se hace extensivo el convenio a este tipo de delitos que se especifican en los artículos 2 al 7 del Protocolo.

- **Capítulo 4**. (Artículo 10 al 16). De nuevo nos encontramos con las disposiciones finales de este tipo de documento, desde la entrada en vigor a las políticas de adhesión y la aplicación territorial.

El Convenio está ratificado por 23 países de la Unión Europea, de los 28 miembros faltan por ratificarlo Grecia, Irlanda, Luxemburgo, Polonia y Suecia.

3.3. Jurisdicción Española

Lo primero es ver a quien afectan y donde las leyes españolas, la referencia en este sentido es el Título I de la Ley Orgánica del Poder Judicial, en concreto el artículo 23 que afirma:

"1. En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte.

2. También conocerá la jurisdicción española de los delitos que hayan sido cometidos fuera del territorio nacional, siempre que los criminalmente responsables fueren españoles o extranjeros que hubieran adquirido la nacionalidad española con posterioridad a la comisión del hecho" (26)

Además de estos dos supuestos hay otros supuestos que dependen del tipo de delito.

(26) **BOE.** *LOPJ.* 1985.

La legislación aplicable a delitos relacionados con el ciberdelito es variada, a continuación vemos una tabla con los delitos y su reflejo en el código penal español:

Delito	Artículos del Código Penal	Resumen
Acceso Ilícito	Artículo 286	Castiga el acceso ilegitimo, y facilitar este. También la modificación de equipos para acceso ilegitimo y el uso de estos.
Contra la libertad sexual	Artículos 187, 189	Castiga la provocación sexual y la prostitución.
Pornografía Infantil	Artículo 189	Se castiga utilizar menores con fines exhibicionistas o pornográficos. Así como producir, vender o exhibir estos materiales.
Falsedad Documental	Artículos 390, 396 y 400	Se castiga la alteración de un documento y la simulación ilegítima
Publicidad engañosa	Artículo 282	Se castiga la publicidad con objeto de engañar al consumidor.
Revelación de Secretos	Artículo 278	Se castiga la revelación de información personal.
Contra el patrimonio	Artículos, 252, 253, 254, 255, 256	Se castigan las estafas, la apropiación indebida y los fraudes
Interceptación y derecho a la intimidad	Artículo 197	Se castiga el robo de correos electrónicos, documentos personales y telecomunicaciones.
Estafas informáticas	Artículo 248	Castiga la fabricación de software destinado a la comisión de estafas.

Usurpación de identidad	Artículo 401	Castiga la usurpación del estado civil de una persona. (Ver delitos de Falsedad Documental.)
Terrorismo	Artículos 571 - 580	Castiga la pertenencia o colaboración con algún grupo terrorista.
Propiedad Intelectual e industrial	Artículos 270, 271, 272	Castiga el que plagie, distribuya o comunique una obra literaria, artística o científica si hay ánimo de lucro.

Como vemos gran cantidad de delitos se ven reflejados en el código penal español, aunque muchas veces no de forma específica o con lagunas que pueden lugar a problemas a la hora de enjuiciar al que comete un delito.

CAPÍTULO 4.
TÉCNICAS USADAS EN EL CIBERCRIMEN

4. Técnicas usadas en el cibercrimen

Cuando hablamos de cibercrimen, hablamos de como los delincuentes utilizan la red para cometer delitos,

En un primer momento, cuando los medios de espionaje eran más limitados, el simple uso del correo electrónico o sistemas de chat eran suficientes para permanecer ocultos en la red, pero con el avance de los sistemas de investigación y persecución de delincuentes estos han tenido que ocultarse en la red. Cuando hablamos ocultarnos para cometer un cibercrimen surgen siempre dos conceptos**, red oscura** (darknet) **y red profunda** (Deep Web).

Al hablar de red profunda hablamos de lo expuestos o accesibles que están los datos a través de Internet, no de si su origen o fin es legítimo. Actualmente se estima que la red profunda, es decir, la parte de Internet que no es pública y accesible supone un 96% de la red. Mientras que la red de superficie (Surface Web) sólo ocupa ese pequeño 4% restante. Ese 96%

Por tanto hablar de cibercrimen y técnica es hablar de **red oscura** (darknet). El concepto lo acuñaron en 2002 un grupo de investigadores de Microsoft en el documento "The Darknet and the Future of Content Distribution" (Peter Biddle, 2002), la red oscura afirman se basa en tres supuestos:

- Cada objeto distribuido estará disponible para una fracción de usuarios de forma que puedan copiarlos.
- Los usuarios copias objetos si es posible y les interesa.
- Los usuarios están conectados a redes de banda ancha[23].

La red oscura emerge de la inyección de objetos de acuerdo a la primera afirmación, y la distribución de estos cumpliéndose la segunda y la tercera afirmación. Uno de los pilares de la red oscura es el hecho de que todo sistema la puede proveer de contenido porque hay un determinado grupo de usuarios que serán capaces de sobrepasar los mecanismos de seguridad.

[23] El concepto banda ancha varía con los años. Una de sus características más importantes es la posibilidad de estar siempre conectado (conexión permanente) y baja latencia y alta capacidad. La ITU afirma: "la banda ancha es capaz de entregar de manera fiable servicios convergentes y de ofrecer simultánea y conjuntamente voz, datos y vídeo, posiblemente a través de redes diferentes" (38)

No toda la información robada acaba en la red oscura, en ocasiones la información militar, industrial o los secretos personales tienen más valor si no son difundidos.

Aunque a priori este tipo de redes parecen estar concebidas para el delito, también se utilizan con el fin de mantener la privacidad en las comunicaciones. Es más, herramientas como TOR afirman estar creadas con este fin.

Se considera que hay dos tipos de red oscura, las redes oscuras peer to peer y las no peer to peer.

4.1. Redes oscuras peer to peer

Dentro de las redes oscuras peer to peer podemos diferenciar dos tipos, las conocidas como redes peer to peer anónimas y las conocidas como amigo a amigo.

Las **redes peer to peer anónimas** se conocen así porque tanto sus usuarios como sus nodos son pseudoanónimos, es necesario que los nodos tengan un pseudónimo para poder llegar a ellos, aunque en principio esto no debe influir en el anonimato de los host. Las **redes amigo a amigo** (friend to friend) son totalmente anónimas, los usuarios sólo se conectan con equipos previamente conocidos. Este tipo de redes permiten la transmisión libre de la información.

Debido al funcionamiento de Internet, ciertos grupos están desarrollando redes oscuras fuera del control de Internet, generalmente en zonas limitadas y a través de WiFI se consigue montar una red paralela a Internet con gran capacidad para compartir información.

4.1.1. Freenet

Freenet es la red oscura peer to peer más usada, es totalmente distribuida y anónima, está diseñada como un almacén de datos distribuido, se han construido sobre ella un gran número de aplicaciones que permiten por ejemplo la publicación de una página web de forma anónima y distribuida.

Es prácticamente imposible eliminar un contenido, ya que la información está distribuida, lo que es un auténtico quebradero de cabeza cuando se tratan de ficheros delictivos, como puede ser pornografía infantil, sin embargo es una gran herramienta cuando lo que se quiere es evitar la censura.

Funcionamiento:

Cada nodo posee una caché visible información, la información que más se solicita es la que más se replica.

Cuando se accede a información, se replica en cada uno de los nodos que atraviesa hasta llegar al que ha hecho la petición.

Cuando un nodo se queda sin espacio, se elimina la información que ha sido accedida en menos ocasiones.

Tiene un sistema de publicación muy similar a WWW. La información está asociada a una clave, que se requiere para acceder a un fichero, de forma similar a la que se hace uso de una URL.

Al estar todos los datos distribuidos, si se quiere que los datos no estén accesibles mediante un ataque DoS es prácticamente imposible.

Freenet utiliza un protocolo NGR (Next Generation Routing) que se adapta a la topología de la red u toma las decisiones de enrutamiento en función de los tiempos de respuesta de los nodos y no de la cercanía.

Funcionamiento del protocolo NGR:

Cada nodo tiene una lista de nodos conocidos iniciales a los que realiza las primeras consultas. En cada petición de información amplía este listado. Se almacena una lista de pares de nodos / clave para mejorar la eficiencia. El protocolo supone que si un nodo tiene información sobre un tema, tendrá más información similar. Las tablas de encaminamiento no se transmiten a otros nodos.

Cuando se recibe una petición pueden pasar dos cosas, que tenga la información, en este caso se envía la información a través de los nodos de los que ha llegado, es decir deshaciendo el camino. SI no tiene la información reenvía la información al nodo que tiene más probabilidad de tener la información.

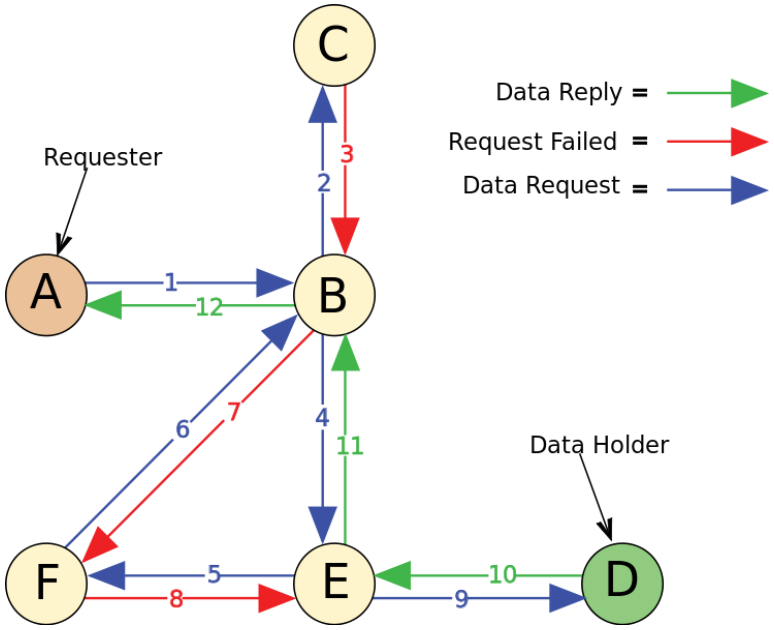

Figura 8. Arquitectura de Freenet. Figura de (27)

Cuando se inserta un fichero, se le asigna una clave única GUID (Global Unique Identifier).

La red utiliza dos tipos de clave:

- **CHK** (Content-Hash Keys): se base en sumas de verificación SHA-1 del contenido del fichero. De esta forma hay una clave única para cada fichero. (Salvo en el caso de que haya una colisión de SHA-1).
- **SSK** (Signed-Subspace Keys): tiene un funcionamiento similar a una URL, primero se genera un par de claves pública y privada. Se elige la descripción del fichero y se hace hashing de la clave pública y de la descripción antes de concatenarlas y volver a hacer hashing de la suma.

Arquitectura:

Tiene un funcionamiento a un i-nodo[24] UNIX, normalmente se utilizan las claves SSK para el almacenamiento de fichero indirectos, estos contiene punteros a los datos auténticos que si son almacenados con CHK.

(27) **XcepticZP.** commons.wikimedia.org. [En línea] http://commons.wikimedia.org/wiki/File:Freenet_Request_Sequence_ZP.svg.

[24] Es una estructura de datos propia de los sistemas de ficheros UNIX, un i-nodo guarda las características de un archivo, como permisos, fechas o la ubicación). Pero no guarda el nombre del fichero,

Si un usuario actualiza un fichero, se obtiene un nuevo CHK. El propietario actualiza los SSK con el nuevo CHK. La versión sigue disponible con el antiguo CHK.

Problemas de Freenet:

Como no se sabe quién tiene los datos, se puede inundar la red de peticiones hasta que llegan al nodo adecuado, esto lo controla con el tiempo de vida y la detección de bucles (si a un nodo le llega la misma petición desde dos nodos diferentes le indica a uno de los dos que por ese camino no va a encontrar los datos).

Las actualizaciones de documentos antiguos pueden inundar la red con mensajes de actualización.

4.2. Redes oscuras no peer to peer

Las redes oscuras no peer to peer necesitan de servidores que controlen el funcionamiento de la red, no bastan sólo los nodos finales como hemos visto en las redes peer to peer. Actualmente sólo hay una red lo suficientemente estable y en uso como para que merezca ser estudiada, es el caso de TOR.

4.2.1. TOR

Cuando hablamos de ciberdelincuencia, en cualquiera de sus formas, en la mayoría de los casos nos encontramos con un punto común. La ocultación a la hora de cometer el delito, y en este ámbito sin duda la red TOR constituye un estándar de facto. Como me hemos visto anteriormente TOR se considera una *darknet*, es como vemos la más extendida.

TOR está formado básicamente por dos elementos, los Router Onion, los Proxy Onion y los servidores de directorio, aunque estos suelen estar integrador en los mismo Router Onion.

Router Onion: son los encargados de encaminar la información. Mantienen una conexión activa con cada uno de los demás router Onion, normalmente las conexiones entre routers se mantienen activas, aunque pueden ser cerradas si se sobrepasa un determinado tiempo de inactividad.

Proxy Onion: normalmente en el propio equipo origen, su función es hacer una petición al servicio de directorio y posteriormente establecer circuitos a través de la red. También se encarga de controlar las peticiones que llegan desde las aplicaciones: aceptan flujos TCP y los multiplexa a través de los router Onion.

Las conexiones entre los proxy y los router no son permanentes. Si no hay circuitos ejecutándose sobre la conexión se cierran.

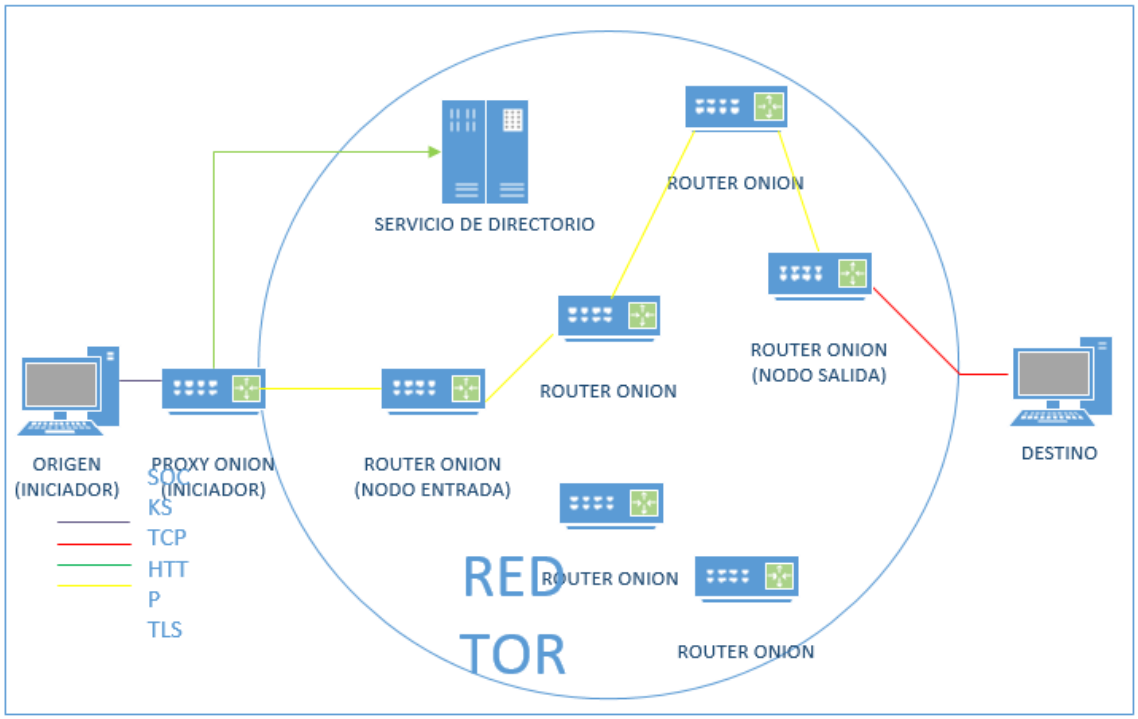

Figura 9. Esquema básico de componentes de la red TOR

Arquitectura actual de TOR

Hablamos de la arquitectura actual de TOR, porque podemos decir que está viva, actualmente está en continuo debate, para la mejora del rendimiento.

Cuando hacemos una petición a una página web, lo primero que hacemos es una petición a un servidor DNS, además de la http, por tanto el tanto las peticiones http como DNS tienen que ser enviadas directamente a la red TOR.

En principio cualquier aplicación que sea capaz de usar SOCKS funcionará sin problema con TOR, las aplicaciones que no funcionen con SOCKS deberán ser "*torificadas*[25]".

Para entender mejor la arquitectura de TOR y los protocolos que usa lo vamos a dividir en dos partes, por un lado lo que se conoce como extensión de circuitos, lo que sería el establecimiento de la conexión y por otro lado el transporte de la información.

[25] Para hacer compatibles con TOR aplicación en sistemas GNU Linux se utiliza el comando Torify, por ello se ha traducido y es de uso común en documentos el concepto *torificar*. En Windows se utilizan otros software como FreeCap.

En las comunicaciones TOR la información se divide en células, estas siempre responden a la misma estructura: tamaño de 512bytes, divididos en una parte de cabecera y otra de datos (payload). La cabecera incluye un identificador de circuito (circID) y un comando que especifica que hay en la parte de datos. En función de este parámetro, nos encontramos con dos tipos de célula, las células de control que siempre son procesadas por los nodos y las células de transmisión[26], que son las encargadas de transmitir los datos.

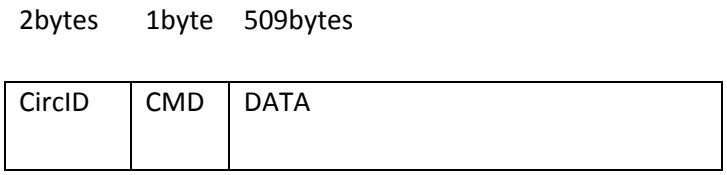

Figura 10. Célula TOR

Tipos de células de control:

- Padding: se usan para mantener el enlace activo enviando mensajes *keepalive*.
- Create y created: usadas para el establecimiento de un nuevo circuito.
- Destroy: usada para cerrar un circuito.

Tipos de células de transmisión:

- Relay data: flujo de datos a través del stream.
- Relay begin: para abrir un stram TCP.
- Relay end: para hacer un cierre ordenado del stream.
- Relay Teardown: para cerrar un stream roto previamente.
- Relay conected: para notificar al proxy que la conexión se ha realizado correctamente.
- Relay extend y relay extended: para extender y confirmar la extensión del circuito en un nuevo salto.
- Relay truncate y relay truncated: para cerrar una parte del circuito y confirmar el cierre.

Extensión de circuitos:

Arquitectura

En la figura vemos las diferentes capas que forman la pila de protocolos usados por TOR para llegar al nuevo nodo, partimos de un circuito formado por el nodo **iniciador** (proxy Onion), que

[26] La literatura sobre TOR habla de este tipo de células como células relay.

forma un circuito con un nodo **intermedio** y con el nodo **previo**, el siguiente paso es conectarse al nodo **destino**.

	Iniciador	Intermedio	Previo	Destino
	Setup		Setup	Setup
	Cell Auth		Cell Auth	
	Circuit	Circuit	Circuit	
TOR	TLS	TLS	TLS	TLS
HOST	TCP	TCP	TCP	TCP
	IP	IP	IP	IP

Figura 11. Pila de protolos Extensión de circuitos TOR

Setup: el protocolo de configuración de TOR es el encargado de establecer y configurar la conexión, está ligado fuertemente a la autenticación extremo a extremo y al intercambio de claves. Es el responsable también del control de congestión.

La capa Setup puede interactuar directamente con la capa TLS cuando el mensaje de control va destinado a un nodo conectado directamente, o a través de las Capas Circuit y Cell Auth cuando hay nodos intermedios.

Cell Auth: la célula de autenticación de TOR se utiliza para proveer una integridad extremo a extremo.

Circuit: es la capa responsable de la confidencialidad. Se encarga de multiplexar y demultiplexar las conexiones realizadas sobre diferentes circuitos sobre TLS y del rendimiento del enrutado basado en etiquetas[27]. Como vemos en la imagen, la pila de protocolos es similar en todos los nodos menos en los intermedios, que sólo llegan a esta capa, las células recibidas se desencriptan, se etiquetan y se enrutan a través de una conexión TLS de acuerdo a una tabla de enrutado.

[27] El enrutado basado en etiquetas sustituye al clásico basado en tablas de asignación. Este enrutado se produce en la capa de enlace de datos, en el protocolo TCP/IP es parte de la capa de enlace (en el modelo OSI es la capa 2). Es el enrutado usado en MPLS.

TLS: la capa de TLS está construida con OpenSSL y es la responsable de proveer la autenticación salto a salto, la integridad y la confidencialidad.

TCP: La capa TCP es la encargada del control de la congestión salto a salto, de la entrega en orden y de la integridad de los datos TLS.

IP: Es la responsable de enrutado IP de los paquetes entre el host y los nodos TOR.

Funcionamiento:

En el caso de la extensión de circuitos, el iniciador primero envuelve el mensaje de control con Cell Auth, dos capas de encriptación (circuit) y envía el paquete a la capa TLS.

Cuando el nodo previo recibe una célula de la capa TLS, la capa final de encriptación es eliminada, la etiqueta de autenticación es verificada y el mensaje de control procesado. El nodo previo puede ver que el mensaje de control indica extensión del circuito (RELAY_EXTEND), y puede enviar un mensaje de control CREATE al nodo destino.

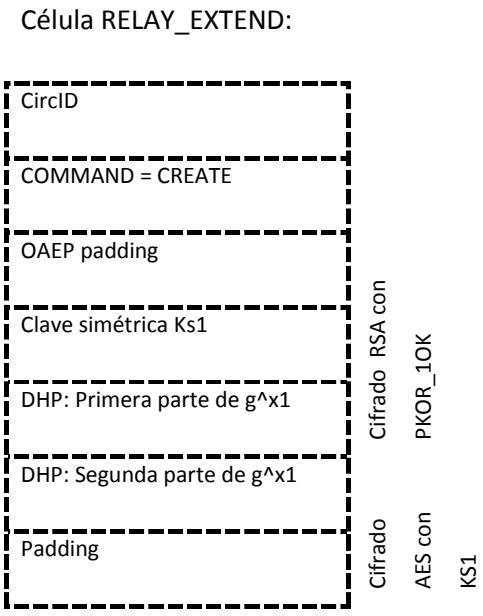

Figura 12. Detalle de la Célula Relay Extend de TOR

Como vemos mezcla cifrados con RSA y cifrados AES con clave pública.

Célula CREATE:

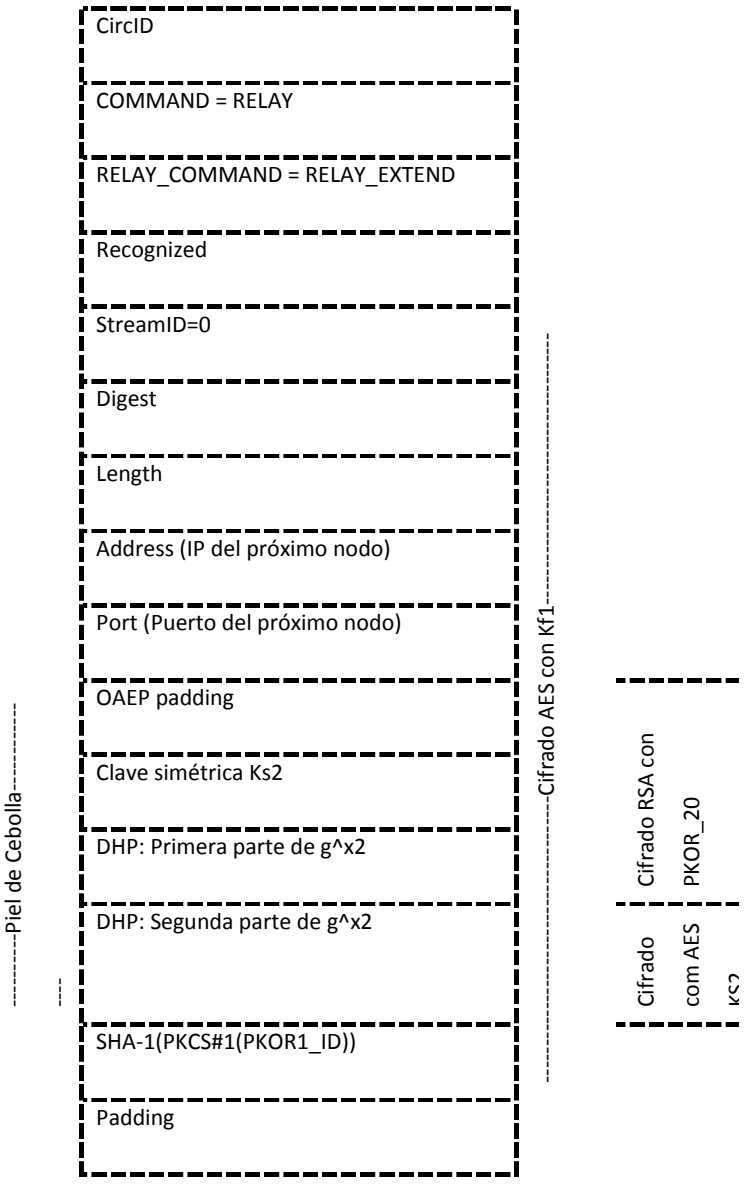

Figura 13. Detalle de la celda CREATE de TOR.

Como vemos mezcla cifrados con RSA y cifrados AES con clave pública. Los campos están cifrados dos veces, al cifrarse lo que es el campo y luego realizarse el cifrado del conjunto de campos.

Establecimiento de la conexión:

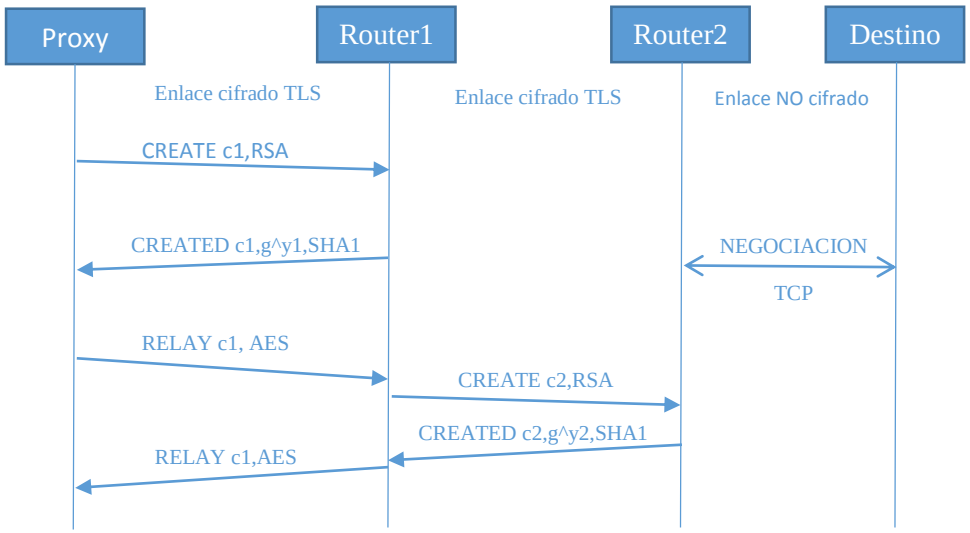

Figura 14. Esquema de establecimiento de la conexión TOR

Como vemos se crea la conexión paso a paso, el último extremo de la conexión se produce con una conexión estándar TCP no cifrada.

Truncamiento de la conexión:

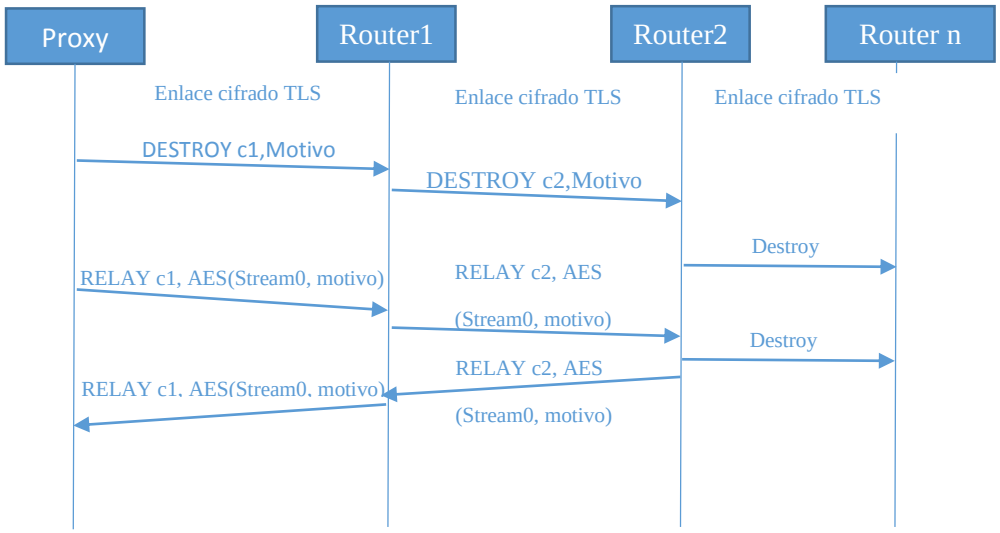

Figura 15. Truncamiento de la conexión TOR

Cuando uno nodo detecta un error irrecuperable o que todas las conexiones se han cerrado y el tiempo de vida a finalizado ordena el cierre con el *destroy*.

Protocolo de transporte de datos:

Arquitectura:

Cuando queremos enviar datos a través de TOR, la arquitectura cambia, un poco, en la siguiente figura vemos cómo quedaría la pila de protocolos.

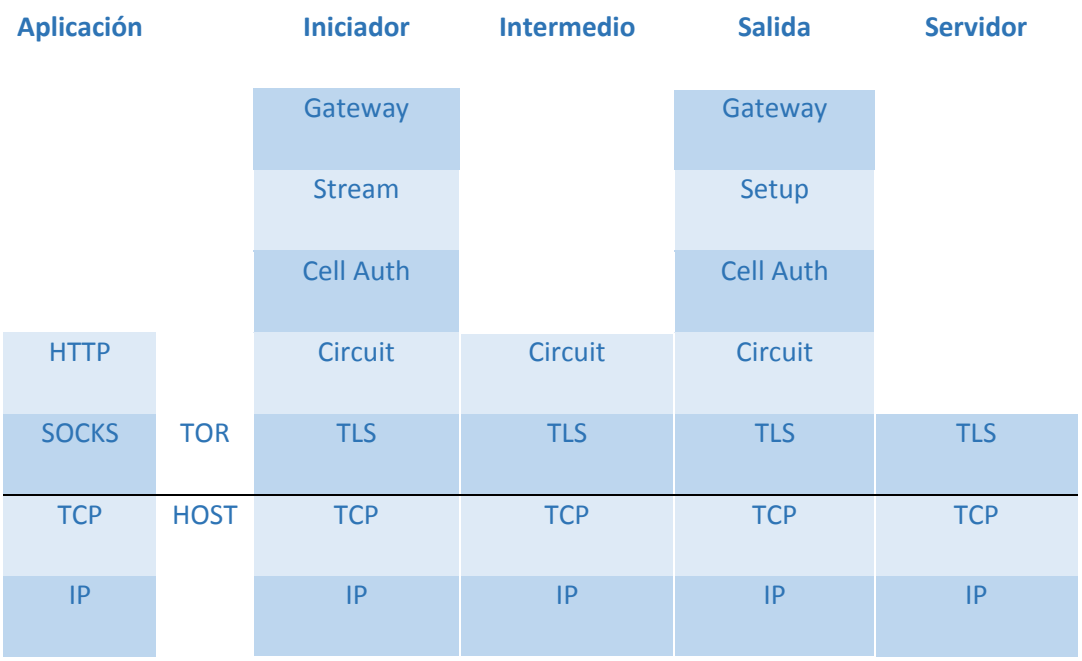

Figura 16. Pila de protocolos para transporte de datos TOR

Los niveles de **Cell Auth**, **Circuit** y **TLS** no varían del supuesto anterior. Los nodos intermedios no pueden distinguir a estos niveles sin células de control o de transporte de datos.

Gateway: en el iniciador, la capa Gateway de TOR recibe paquetes SOCKS[28] desde la capa SOCKS de la aplicación, extrae los datos útiles y divide estos en células. Estas son encapsuladas de la misma forma que los mensajes de control y enviadas al nodo de salida a través de varios intermediarios. Esta capa es también la encargada de multiplexar varias partes de información sobre un solo circuito.

TCP / IP: además de encargarse del transporte de los datos TLS, también se encarga de transportar los datos SOCKS al iniciador TOR.

[28] SOCKS es un protocolo de Internet usado en conexiones cliente-servidor, está pensado para hacer esta conexión cliente servidor a través de un proxy. SOCKS estaría en la capa de sesión del modelo OSI. Según la pila de protocolos IP está en

SOCKS: La capa SOCKS encapsula el flujo de información con su cabecera SOCKS y transporta los parámetros de negociación.

El proceso de transporte:

Se basa en la negociación de SOCKS, el iniciador debe crear y extender circuitos como sea necesario hasta que se establezca el circuito con el nodo de salida.

La capa Gateway en el iniciador que indica a la capa Gateway en el nodo de salida hace una conexión TCP plana al host requerido por el iniciador, y envía el flujo de datos a este.

Funcionamiento:

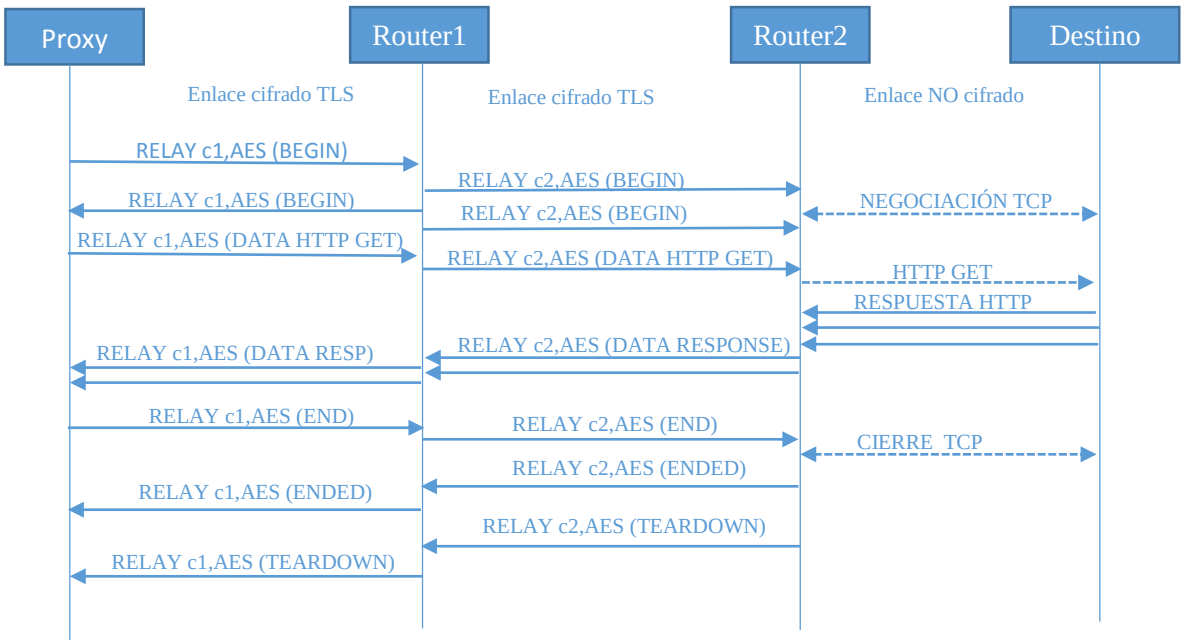

Figura 17. Funcionamiento del transporte TOR

Como vemos en la Figura 17 el proxy elige un nodo de salida que tenga un circuito abierto, asigna un StreamID que no haya sido usado en ese circuito, construye la célula RELAY_BEGIN que incluye el puerto de destino (80 en este caso) y que está cifrado de forma que sólo el nodo de salida es capaz de saber la dirección de destino y la aplicación (puerto). La célula atraviesa los nodos intermedios siendo reenviado el contenido útil. El nodo de salida (Router 2 en el esquema simplificado de la figura) utiliza la dirección y puerto para intentar una nueva conexión tcp con el destino. En el momento del cierre para cerrar un stream se usan los RELAY_END, si el cierre por algún motivo es abrupto se utiliza REALY_TEARDOWN para cerrar el stream.

Algoritmos de cifrado utilizados:

TLS: Usado para el establecimiento de la conexión. La versión utilizada actualmente es TLS/SSL versión 3.

AES: Usado para el cifrado. Se usa AES-CTR con un tamaño de las claves de 128bits.

RSA: Se usa como algoritmo de clave pública. Con claves 1024 bytes y exponente de 65537.

OAEP-MGF1: Usado como esquema de relleno para el RSA.

SHA-1: Se usa como función de resumen del RSA.

Diffie-Hellman: Usado para el establecimiento de las claves.

Pseudodominio de nivel superior[29] .onion:

Este tipo de dominio indica que apunta a una dirección IP anónima sólo por medio de TOR. Las direcciones .onion no son mnemotécnicas como las de DNS, se forman con una combinación de caracteres alfanuméricos generados automáticamente basándose en una clave pública, es un número de 80bit en base32.

4.2.2. Caso práctico: Instalación y uso de TOR

A continuación vamos a ver lo sencillo que es descargar y configurar TOR para una navegación anónima.

Lo primero que vamos a hacer es descargar TorBrowser, el navegador que TOR ha creado especialmente para este cometido en la siguiente dirección:

https://www.torproject.org/projects/torbrowser.html

Encontraremos versiones para los sistemas operativos Microsoft Windows, Mac OS X y Linux en distintos idiomas, entre los que se incluye el español. Una vez que tenemos el ejecutable procederemos a seguir los pasos de su asistente de instalación.

[29] Un pseudodominio de nivel superior es un término usado para servicios que no participan en el sistema DNS oficial pero que usan una estructura y jerarquía similar al de DNS. Normalmente apuntan a equipos que no son accesibles usando el protocolo IP.

Como vemos a continuación es un sencillísimo proceso de tres pasos

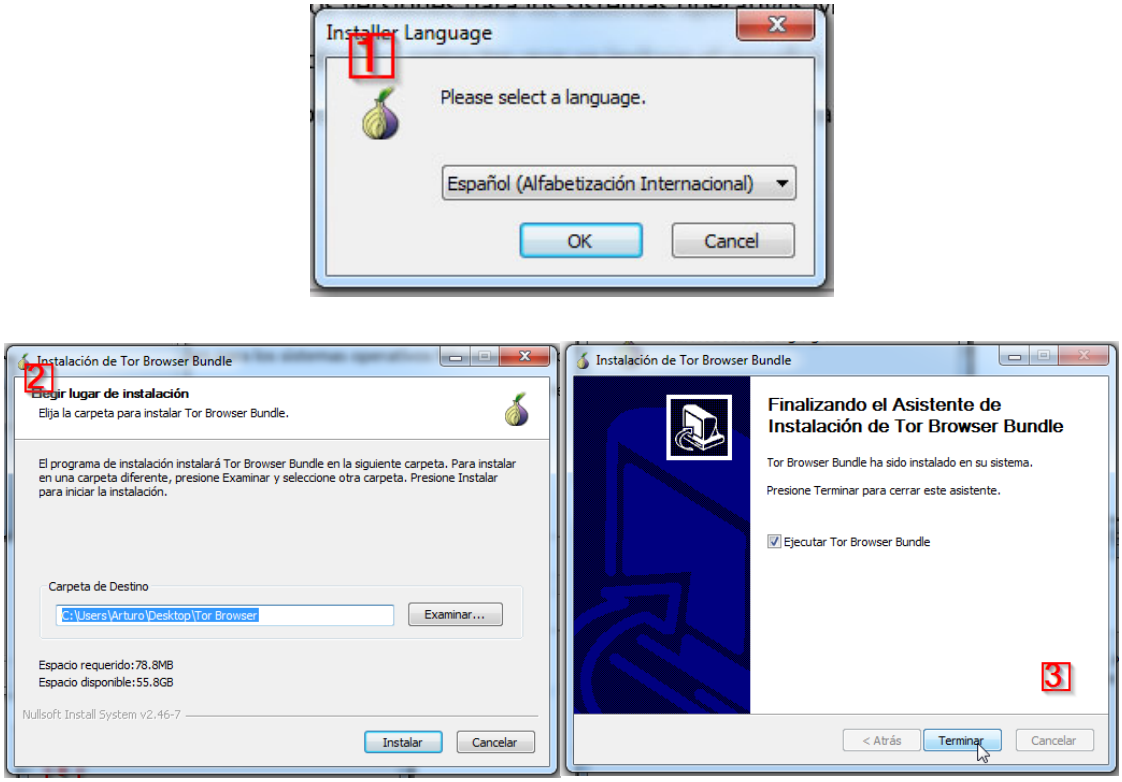

Figura 18. Asistente de Instalación de TOR

Una vez que lo tenemos instalado, en la primera ejecución nos pedirá que lo configuremos, a continuación vemos cómo:

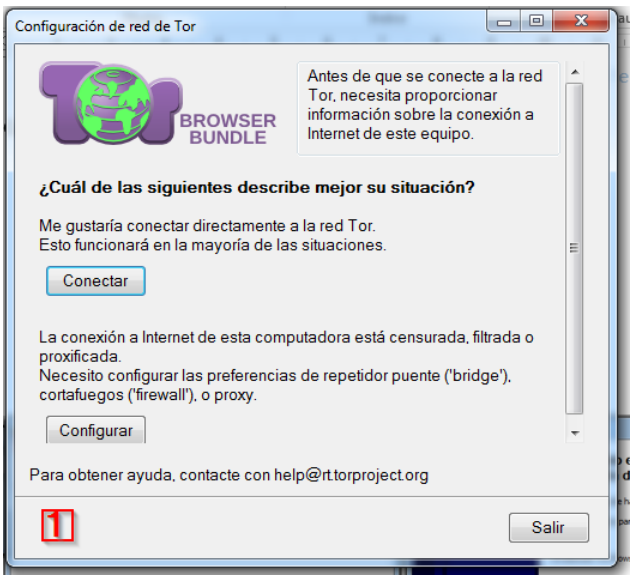

Figura 19. Configurando TOR. Paso 1. Red

Si pulsamos en configurar porque nuestra red atraviesa un firewall o nos conectamos a un proxy, nos pedirá lo siguiente:

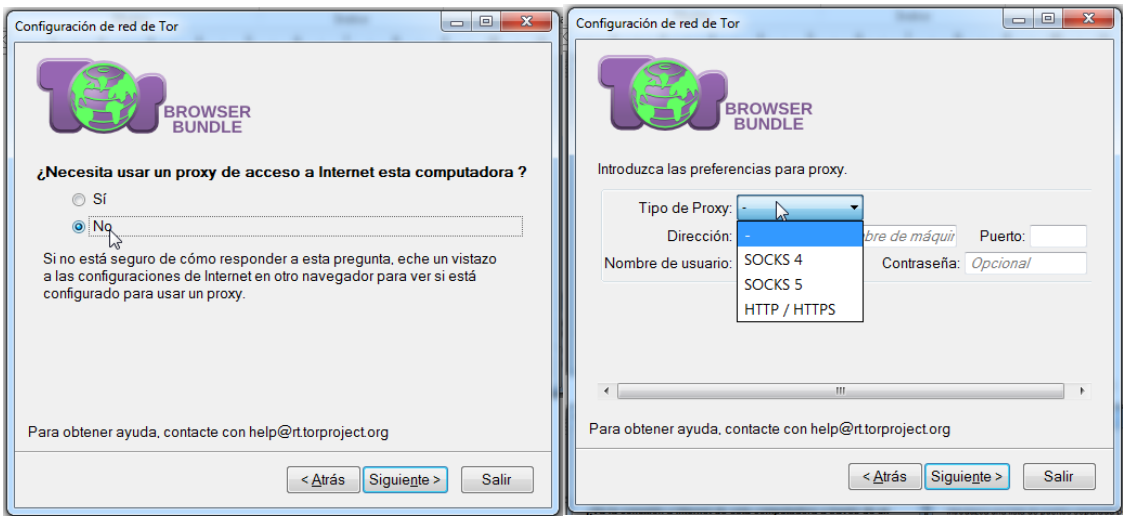

Figura 20. Configuración TOR si salimos a través de un proxy

Si nuestro firewall sólo permite algunos puertos se lo especificamos a TOR, es posible que sólo tengamos permitida la navegación web http, por lo que TOR tendría que funcionar por el puerto 80, su tenemos permitida la navegación web segura https, tendremos abierto el puerto 443.

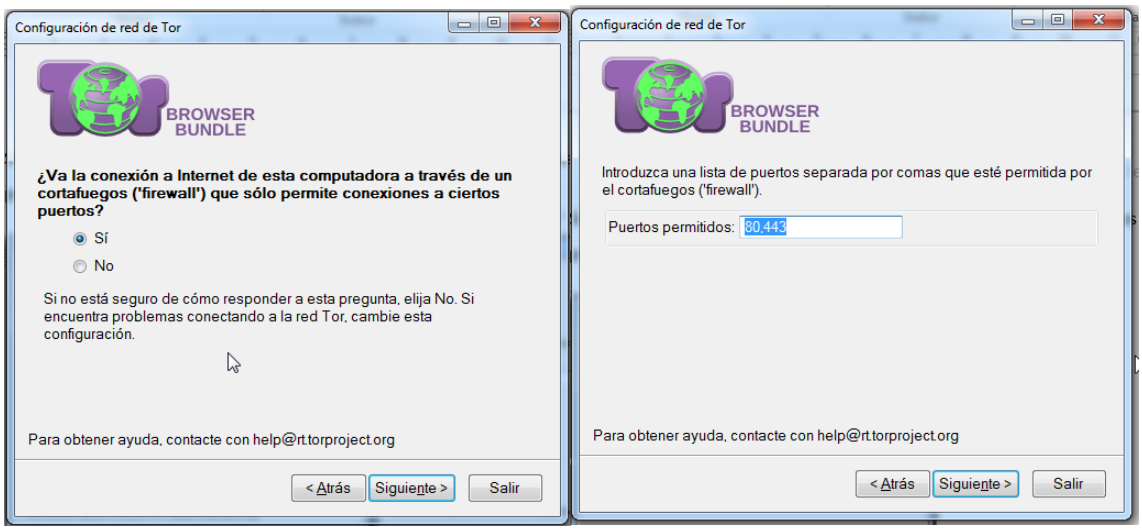

Figura 21. Configuración TOR si salimos a través de un firewall

Es posible que nuestro ISP bloquee TOR, para ello es necesario configurar TOR de la siguiente forma:

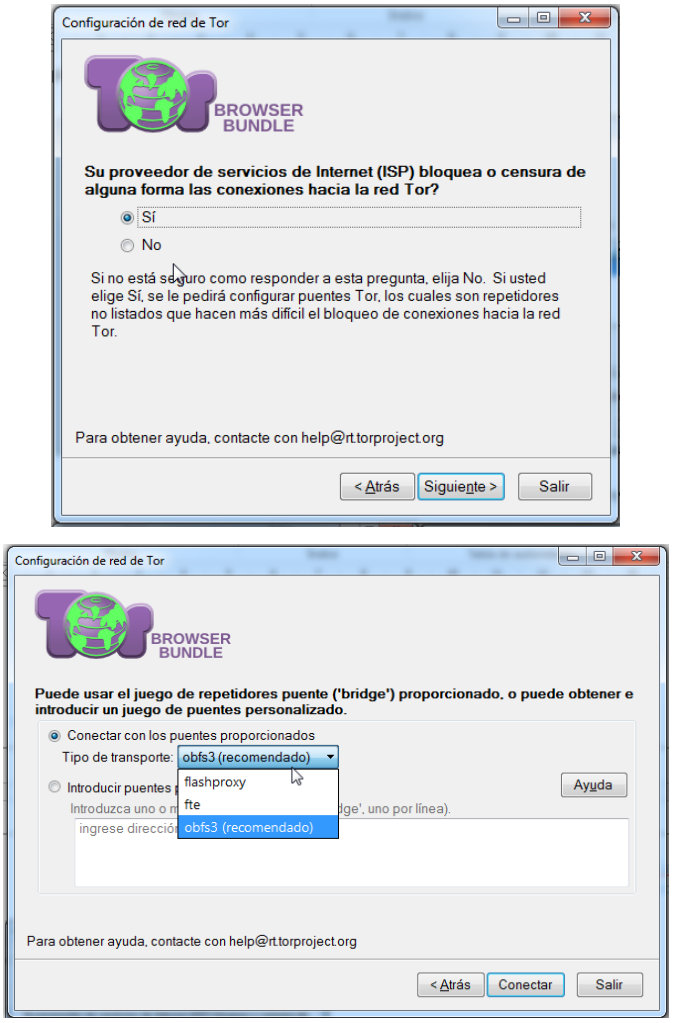

Figura 22. Configuración TOR para bloqueos por ISP

En este caso tendremos que usar un bridge, la propia aplicación viene con alguno de ellos.

Recomienda obfs3[30].

En nuestro caso le damos directamente a conectar, veremos una pantalla de progreso:

[30] Obfs3 es un protocolo de ofuscación para protocolos TCP. La especificación está disponible en https://gitweb.torproject.org/pluggable-transports/obfsproxy.git/blob/HEAD:/doc/obfs3/obfs3-protocol-spec.txt

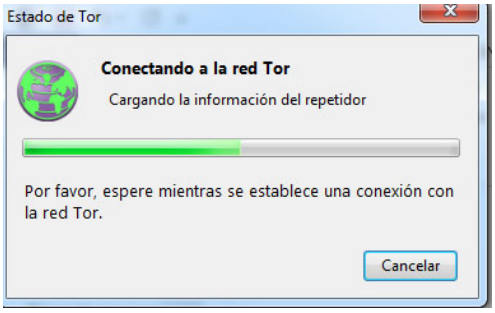

Figura 23. Pantalla de progreso de conexión TOR

Si todo ha ido bien, ya tenemos el navegador funcionando y listo para usar, como vemos su aspecto es similar a Firefox, navegador en el que está basado:

Figura 24. Pantalla de Inicio de TORBrowser

Para comprobar accedemos a la web de la escuela, la cual se carga sin problema, aunque comprobamos que el tiempo de carga es mayor, la navegación es lo suficientemente fluida.

Figura 25. Web de la escuela accedida desde TORBrowser

A continuación vamos a utilizar una página web que nos dice cuál es nuestra IP, de esta forma veremos si realmente hay diferencia llegando desde nuestro navegador habitual o desde TorBrowser. Para esta comprobación usamos: http://bandaancha.eu/mi-ip

Si accedo desde mi navegador habitual obtengo el siguiente resultado:

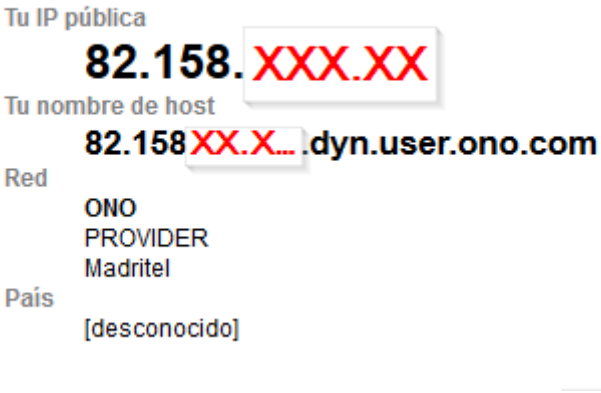

Figura 26. Dirección IP desde FIREFOX

Figura 27. MI IP Desde TOR Browser

Como podemos observar el resultado desde Mozilla Firefox arroja un resultado, que siempre es el mismo y muestra cuál es mi IP real. Sin embargo desde TOR browser el resultado es distinto en cada ocasión, en la Figura 27 vemos que incluso alguno de los host se identifican con servidores TOR. Además la aplicación no es capaz de reconocer la red desde la que se está accediendo, cuando desde Firefox si lo hace.

La otra comprobación que podemos hacer es ver que podemos acceder a direcciones de tipo .onion (Ver punto 4.2.1.).

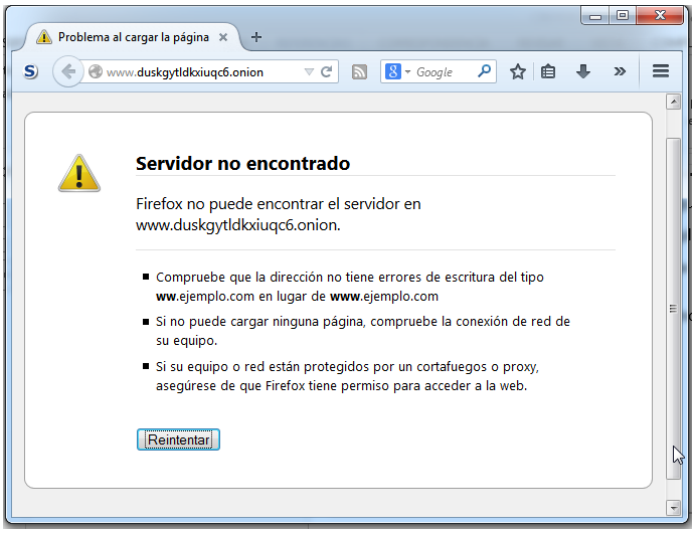

Figura 28. Error en navegación accediendo a dirección .onion desde Mozilla Firefox

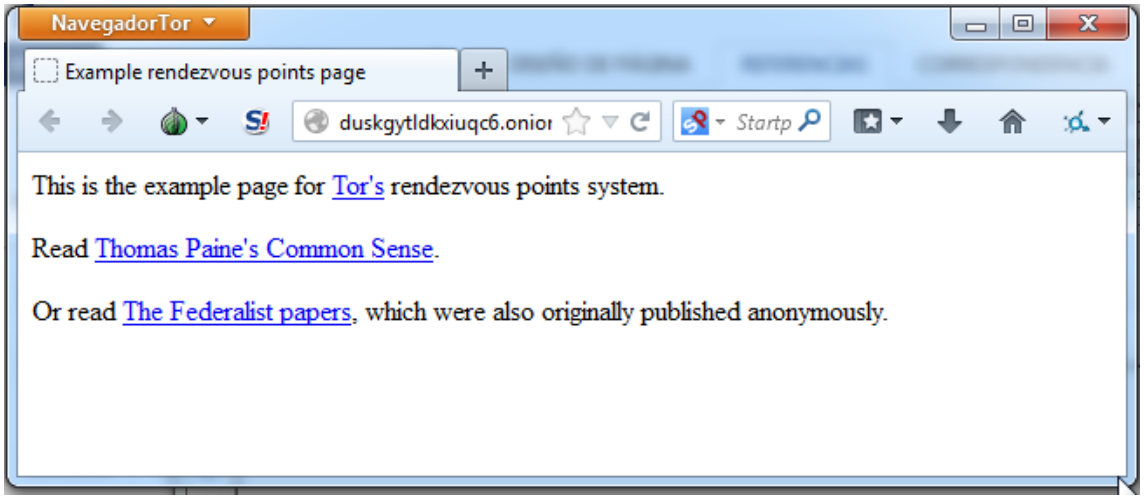

Figura 29. Página de ejemplo dirección .onion desde TORBrowser

Si accedemos desde Firefox obtenemos el típico error 404 de Firefox indicando que el servidor no existe. Firefox no es capaz de llegar a este tipo de página. Sin embargo TOR browser como vemos en la Figura 29 sí que es capaz de ver la página de ejemplo.

Como vemos usar TOR para una navegación privada y anónima es extremadamente sencillo, cualquier usuario puede usarlo.

CAPÍTULO 5.
TÉCNICAS USADAS EN LA DEFENSA Y SEGUIMIENTO DEL CIBERCRIMEN

5. Técnicas usadas en la defensa y seguimiento del cibercrimen

Cuando un particular, gobierno, organismo o empresa piensa en defenderse de la ciberdelincuencia se encuentra con varias soluciones técnicas.

Si queremos hacer segura una red o un equipo lo primero que debemos hacer es definir qué servicios y por lo tanto que puerto y conexiones queremos permitir. En un primer momento es imprescindible la inclusión de un firewall que defina de forma estática que ocurre con lo que entra y sale de la red. Durante mucho tiempo un firewall parecía suficiente para protegerse pero en la actualidad la realidad es que no es suficiente, por ello se necesitan sistemas más avanzados de detección de intrusiones como los IDS y los IPS.

Además de luchar con las intrusiones también es necesario luchar contra otro tipo de ciberdelitos como los ataques de denegación de servicio o los ataques específicos por vulnerabilidades propias de algún software concreto, para ello se utilizan softwares específicos en los servidores expuestos y por supuesto reglas en los anteriormente citados firewalls, IDS o IPS, además en los equipos de usuario se utiliza software antivirus que intentan evitar la ejecución de software malicioso que facilite el acceso a los sistemas o la información.

También se deben proteger las comunicaciones cuando estas salen de nuestro control, es decir, cuando atraviesan Internet. Para proteger las comunicaciones podemos considerar el encriptado de las comunicaciones como algo imprescindible.

5.1. Firewall

Es un dispositivo o simplemente un software que, como mínimo, se encarga de filtrar el tráfico que pasa a través de una Interfaz de red y que decide que ocurre con el tráfico en función de una serie de reglas previamente configuradas.

Aunque en equipos de usuario finales se utilizan firewalls que son un software que monitoriza una única interfaz de red, la realidad es que en redes más profesionales se utilizan equipos específicos con al menos dos interfaces de red que se encargan de procesar el tráfico que las atraviesa. El firewall se sitúa entre la red a proteger y la red interna. Aunque parece lógica esta configuración con dos zonas, cuando tenemos servicios que necesitan estar expuestos al exterior lo normal es que tengamos un firewall con al menos tres zonas. La zona externa

conectada a Internet, la zona interna con más limitaciones (generalmente la red local LAN) y una zona expuesta DMZ (zona desmilitarizada), en la que se incluyen los equipos que necesitan tener una conexión directa al exterior, es el caso típico de servidores web y servidores de aplicaciones web; aunque detrás del firewall esta zona tiene un nivel de seguridad inferior a la de la interior.

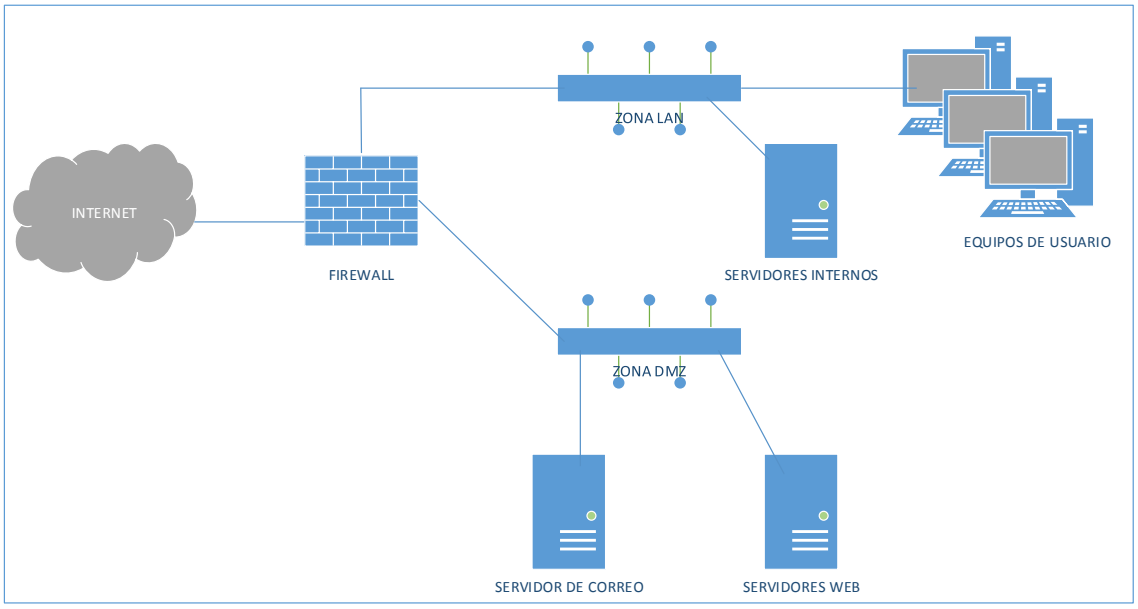

Figura 30. Configuración clásica de configuración firewall

Además de estas funciones normalmente en los firewall se realiza también la función de NAT[31] entre la red interna e Internet, y cada vez más se instalan servicios de VPN[32]. También se puede, aunque es menos común, instalar servicios añadidos de seguridad como un IDS[33].

El **filtrado** normalmente lo que hace es función de esta configuración decidir si un paquete se modifica, se descarta o se deja pasar.

Normalmente se decide a priori lo que se puede y lo que no se puede hacer, normalmente la política más razonable es prohibir todo y a través de reglas abrir los puertos y protocolos que sean necesarios. Cuanto menos puertos se abran más seguro será el firewall.

[31] NAT – Network Address Translation. Se usa para intercambiar paquetes en redes que asignan direcciones incompatibles. El funcionamiento básico es la asignación uno a uno de una IP interna y una IP externa. Esta asignación puede ser estática o dinámica.
[32] Ver punto 5.5.7 de este documento.
[33] Ver punto 5.2. de este documento.

Las reglas se especifica desde que zona a que zona se realiza la conexión, el protocolo utilizado, el puerto de origen y el puerto de destino y que se debe hacer en el caso de que se cumplan estos requisitos.

El orden en que se colocan las reglas en los ficheros de configuración es realmente importante, ya que la mayoría de sistemas firewall en su funcionamiento solo aplican la primera regla que cumple las condiciones, el resto de reglas no se miran en el momento que hay una coincidencia.

Tipos de reglas básicos:

- *Aceptar*: se acepta que el paquete pase a través del firewall desde la zona origen a la zona de destino.
- *Descartar*: el paquete no es aceptado para pasar a través del firewall, el paquete se descarga sin más cortando la comunicación.
- *Rechazar*: al igual que cuando se descartan los paquetes, el paquete es descartado, pero la diferencia es que en este caso si se notifica al host que ha iniciado la conexión que le paquee ha sido rechazado.
- *Redirección*: sirve para redirigir paquetes a un equipo concreto de la LAN o la DMZ.
- *Enmascarado*: hace la función de NAT, es decir, convierte la dirección pública en privada o al revés.
- DNAT: al igual que NAT realiza una conversión ip pública-privada, pero en este caso lo hace en función de la aplicación de destino (puerto de destino).
- *Log*: el firewall guarda información de determinada transmisión en un fichero.

5.2. Detección y protección de intrusiones

Actualmente se ha estandarizado el uso de sistemas que permiten detectar y prevenir intrusiones, aunque no son incompatibles, debido a su complejidad tanto en la implementación como en el manejo diario de los avisos, lo normal es que se elija entre uno de los dos.

El principal problema de estos sistemas suele ser su fase de implementación, ya que al ser sistemas "inteligentes" que van aprendiendo, en una primera fase es normal que haya falsos positivos y bloqueos de conexiones legítimas.

5.2.1. Sistemas de detección de intrusiones (IDS)

Los sistemas de detección de intrusiones, más conocidos por su acrónimo en inglés IDS, **I**ntrusión **D**etection **S**ystem, son sistemas software que mediante sensores virtuales son capaces de monitorizar el tráfico de la red y los accesos a los equipos para evitar posibles intrusiones.

Mediante la información acumulada como patrones de ataque, la definición de lo que es normal en un equipo, por ejemplo las horas en las que un administrador se conecta, los puertos usados y a que puertos se hacen las conexiones, el ancho de banda utilizado, bases de datos de vulnerabilidades conocidas y como se atacan, y por supuesto reglas prestablecidas, un IDS es capaz de detectar un ataque. Podemos entonces hablar de dos tipos de detección, **heurística**, es decir, determinando qué es normal; y **por patrón** para reconocer los ataques conocidos.

Los IDS para ser efectivos tienen que tener añadida la funcionalidad de firewall, ya que de nada sirve detectar las intrusiones si no somos capaces de actuar contra ellas. Esta funcionalidad puede ser integrada con el propio IDS o modificando las reglas del firewall ya existente, este tipo de IDS se denominan **reactivos**. También hay IDS **pasivos** que simplemente avisan o almacenan en una base de datos el posible ataque.

Como vemos a continuación se considera que hay varios tipos de IDS, pero en realidad, para que un IDS sea realmente efectivo es necesario considerar los diferentes tipos como componentes de nuestro IDS.

Hay tres tipos de IDS:

- **Detección de intrusiones de red (NIDS[34])**

Se instalan en el segmento de red a vigilar, en un analizador de paquetes de red (sniffer). Conectado a la red en modo promiscuo absorbe todo el tráfico de red para después procesarlo y mediante reglas definidas y procesos estadísticos detectar los posibles ataques.

[34] Network Intrusion Detection System

Normalmente este procesamiento es analizado en tiempo real, aunque el tráfico puede ser almacenado para su posterior análisis.

Cuando queremos monitorizar una red con NIDS, una de las primeras decisiones que debemos tomar es dónde colocamos el NIDS:

Delante del firewall: como gran ventaja de esta colocación, el NIDS está antes de toda la red y es capaz de detectar los problemas antes de que lleguen siquiera al firewall que sería el primero en estar expuesto. La desventaja de esta colocación, es que el tráfico llega sin ningún tipo de filtro y el tamaño de los logs hace que los requerimientos de la máquina sean muy grandes.

Detrás del firewall: al estar detrás del firewall sólo analiza el tráfico que realmente ha entrado en la red. Este tipo de conexión tiene la dificultad de que podemos tener más de una zona detrás del firewall, como ocurre por ejemplo con la típica configuración con una zona LAN y otra DMZ. La otra desventaja de este tipo de conexión es que el firewall no está protegido por el NIDS.

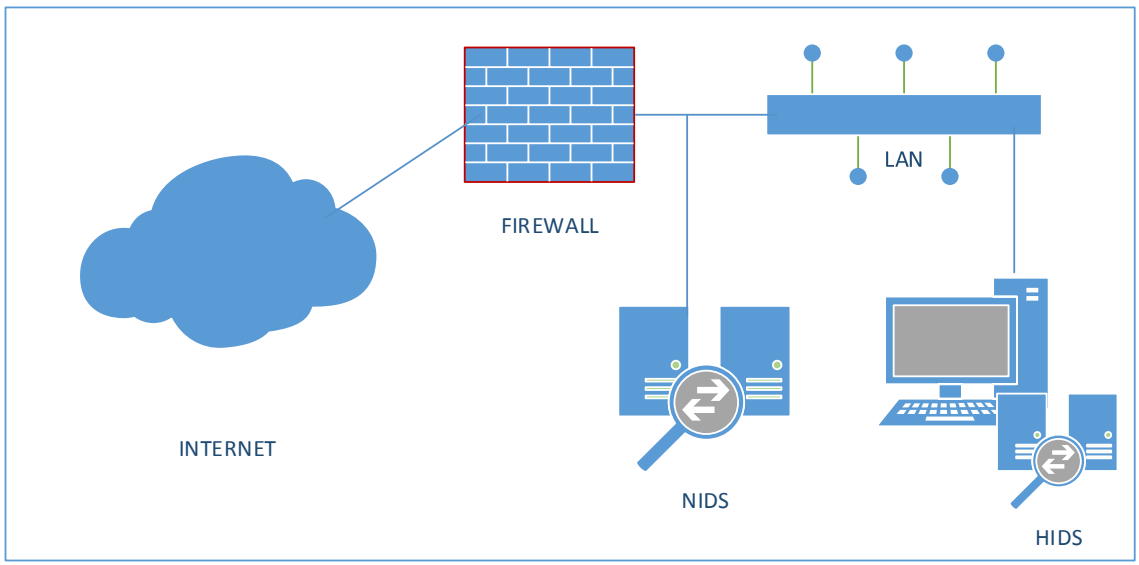

Figura 31. Conexión NIDS detrás del firewall

Delante y detrás del firewall: tendríamos doble nivel de IDS, pero necesitaríamos dos máquinas y si manejamos las mismas reglas en los dos, probamente no sea óptimo en cuanto a recursos. En este tipo de configuración lo idóneo sería la conjunción de un IDS y un IPS. Uno a cada extremo del firewall.

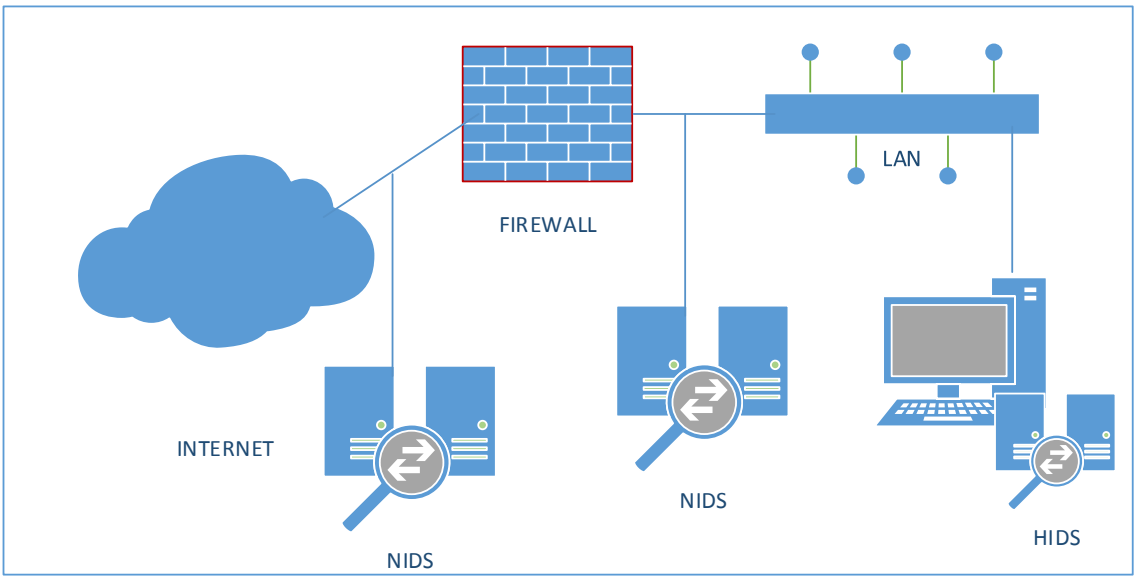

Figura 32. Conexión IDS delante y detrás del firewall

Integrado en el firewall: esta configuración es probablemente la más sencilla, mantiene al firewall expuesto y necesita una máquina más potente que cualquiera de las anteriores configuraciones.

Una vez decidida la posición en la red debemos conectar correctamente el IDS. Si el firewall está integrado en el firewall o conectado a una de sus interfaces de red por las que pasa todo el tráfico no deberíamos tener problema. Si por el contrario lo vamos a conectar a un determinado segmento conectado a un switch, debemos tener en cuenta que un switch, cada vez más inteligente, llegando incluso a niveles 4 de la torre OSI, no reenvía todos los paquetes a todos los puertos como hacían los ya obsoletos HUB. Por ello debemos usar switch que tenga un puerto específico de replicación[35] (port mirroring), estos puertos son configurables, y pueden recibir todo el tráfico que pasa por el switch o el de una VLAN específica si así se configura.

[35] Cada fabricante llama a este puerto de una manera específica. Por ejemplo Cisco Systems lo llama SPAN (Switched Port ANalyzer) o RSPAN (Remote Switched Port ANalyzer), 3COM lo llama RAP (Roving Analysis Port).

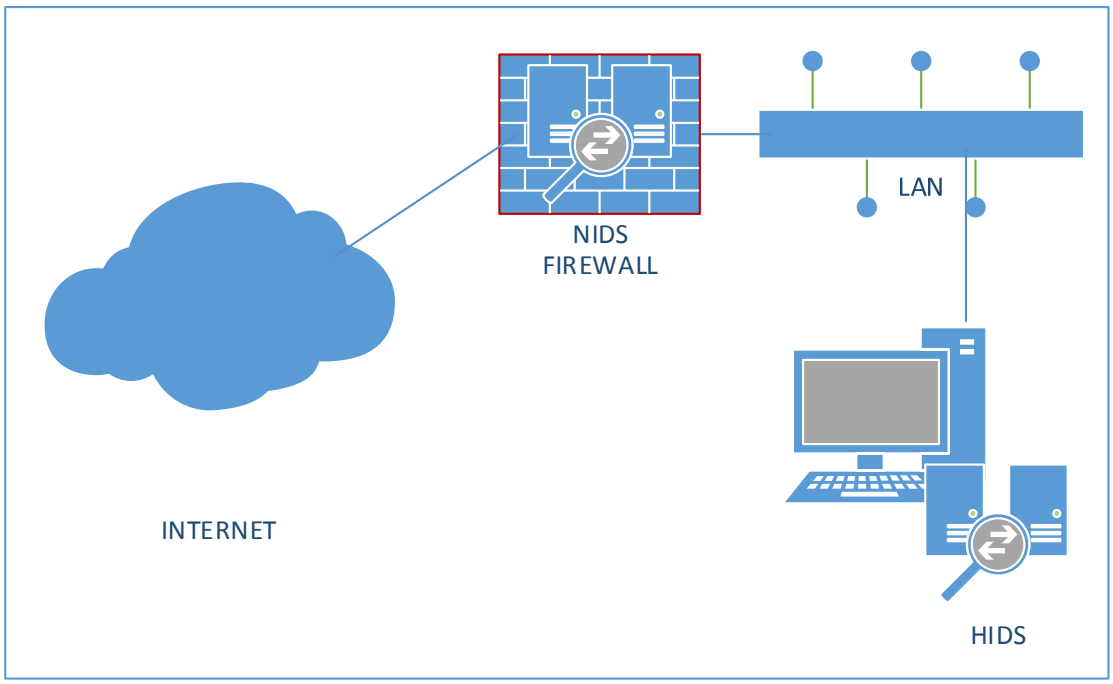

Figura 33. NIDS Integrado en el firewall

- **Detección de intrusiones de nodo de red (NNIDS[36])**

Es similar al detector de intrusiones de red, aunque en este caso sólo se vigila un determinado segmento de red, generalmente el destinado a una VPN o a una zona expuesta, como puede ser donde se encuentra situado un honeypot[37]. El uso de honeypots tiene dos funciones para el administrador de sistemas, por un lado que el atacante se distraiga y pierda el tiempo en sistemas sin importancia, e imprescindible en el caso de un IDS recopilar datos de quien y sobre todo, cómo se realiza un determinado tipo de ataque. De esta forma el IDS va aprendiendo.

- **Detección de intrusiones de host (HIDS[38])**

Para detectar las intrusiones en un host, más allá de comprobar los ataques de red, se recurre a realizar instantáneas de las partes críticas del sistema. De esta forma se puede comparar en tiempo real y hacer saltar las alarmas cuando determinados ficheros del sistema son

[36] Network Node Intrusion Detection System
[37] Un Honeypot es un equipo o conjunto de equipos destinado a atraer un ataque. Normalmente se utilizan equipos con vulnerabilidades conocidas o menos medidas de seguridad.
[38] Host Intrusion Detection System

modificados o eliminados. Normalmente para saber si un archivo ha sido modificado se recurre a sumas de verificación, que mediante algoritmos criptográficos como MD5 nos aseguran con una probabilidad de error mínima (colisiones de hash[39]) si un fichero ha sido modificado. Además de buscar ficheros modificados los HIDS comparan los registros del sistema contra una base de datos de registros con peculiaridades de estos cuando se produce un ataque.

5.2.2. Sistemas de prevención de intrusiones (IPS)

Este tipo de sistemas, funcionan en tiempo real para prevenir que se filtre cualquier intrusión, cuando se detecta cualquier paquete sospechoso se detiene la conexión relacionada. Al contrario que los IDS esta tecnología no se limita a escuchar y mandar alertas, se considera una mejora de los sistemas firewall.

El IPS funciona a nivel de la capa 7 del modelo OSI, tiene la capacidad de descifrar HTTP, FTP y SMTP, los sistemas tienen reglas similares a las de los Firewall.

El IPS no utiliza las direcciones IP, permite poner reglas, pero de un tipo distinto al de los firewall, este tipo de normas detallan el acceso de usuarios a aplicaciones y equipos.

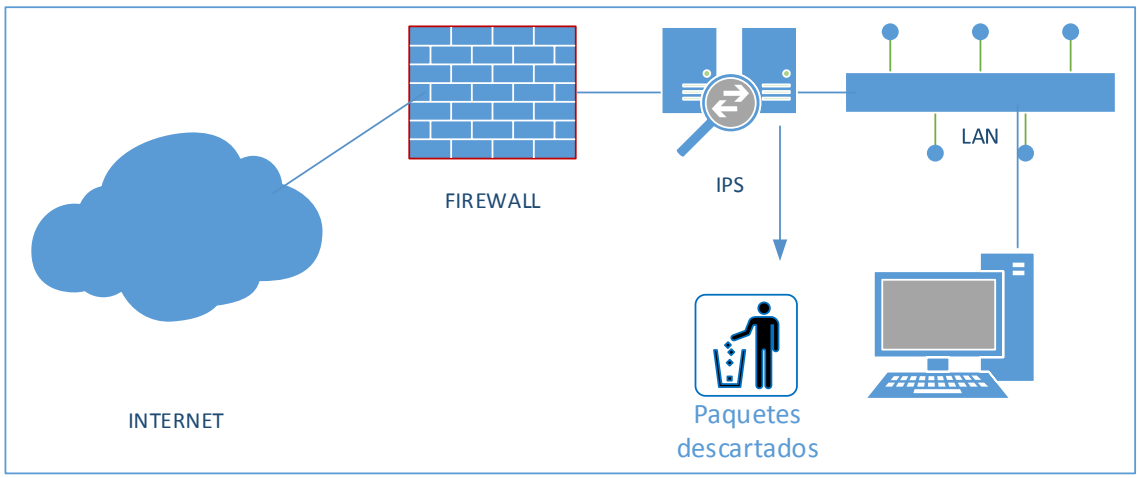

Figura 34. Esquema de conexión IPS

[39] Se produce una colisión de hash cuando dos entradas distintas de una función hash dan lugar a la misma salida.

Tipos de IPS:

- **HIPS – IPS basados en Host**

Es un software que monitoriza un único equipo de actividad sospechosa. Sólo es capaz de analizar lo que ocurre en el equipo que está instalado, de una forma parecida al funcionamiento de un software antivirus convencional en un equipo de usuario.

Lo mínimo que debe monitorizar y prevenir es:

  - Que se obtenga el control de otros programas
  - Que se modifiquen claves del registro importantes
  - Que se finalicen algunos programas, como el software antivirus
  - Que se instalen dispositivos o drivers
  - Que se acceda a la memoria

Si se detecta alguno de estos fenómenos se bloqueará la conexión desde la que se esté realizando el ataque.

- **NIPS – IPS basados en Red**

  Este tipo de IPS es un hardware, o una instalación software en un equipo específico, en algunos casos podría ser parte del firewall de red.

  Analizan, detectan e informan de eventos relacionados con la seguridad, están pensados para inspeccionar el tráfico y la configuración de las políticas de seguridad.

- **WIPS – IPS Wireless**

  Monitoriza en una red inalámbrica buscando tráfico sospechoso analizando los protocolos de red Wireless.

- **NBA – Análisis del comportamiento de red**

  Examina el tráfico de red para identificar hilos que generan flujos de tráfico inusuales, como puede ser un ataque DDoS, ciertas formas de malware y violaciones de políticas.

Métodos de detección

La mayoría de los IPS conocidos usan los siguientes tres métodos:

- **Detección Basada en firmas:** el IDS monitoriza paquetes en la red y compara con patrones de ataques preconfigurados y predeterminados como firmas. Es un funcionamiento similar a la detección basada en firmas de los sistemas antivirus.
- **Detección basada en anomalías estadísticas:** la detección basada en estadísticas determina el funcionamiento normal de la red, como puede ser el ancho de banda usado normalmente, que protocolos se usan, que puertos y dispositivos se conectan generalmente a otros.
- **Análisis de estado del protocolo:** este método identifica desviaciones del estado del protocolo mediante la comparación de eventos observados con determinados perfiles que son generalmente aceptados como actividad legítima.

5.3. Sistemas anti ataques DDoS y vulnerabilidades

Un ataque de denegación de servicio (DoS) es un intento de hacer que un recurso conectado a Internet no esté disponible, normalmente de forma temporal. Un equipo provoca tantas peticiones que no sobrecargan el sistema atacado. Este tipo de ataque ha evolucionado con el tiempo y lo normal es que se haga de forma distribuida, ya que es mucho más difícil de combatir. Un ataque DoS en muchos casos es tan fácil de combatir como bloquear una IP.

Un ataque DDoS es un ataque de denegación de servicio distribuido, más conocido por ataque DDoS (por sus siglas en inglés: Distributed Denial of Service).

5.3.1. Botnets

Antes de ver cómo funciona un ataque de denegación de servicio, vamos a ver qué es y cómo funcionan las botnets, ya que estas se utilizan en la mayoría de los ataques DDoS.

Una botnet es una red de ordenadores u otros dispositivos comprometidos, estos dispositivos infectados con algún tipo de malware, lo que les pone a disposición del atacante.

Actualmente tiene una arquitectura con tres actores, el “botmaster” es el atacante, el que controla la red, el servidor de control y comandos es al que se conectan los equipos infectados y quien tiene la capacidad de darle órdenes a los equipos infectados.

Para las redes centralizadas, normalmente se utilizan mecanismos pull, por ejemplo en las botnet basadas en HTTP el botmaster publica los comandos en una página web, los equipos infectados se conectan periódicamente a la página para ver si actualizaciones de los comandos. La dirección de la web es fija, pero puede ser cambiada por uno de los comandos. Otra forma común de enviar los comandos, y la que más se ha usado es publicar los comandos en un determinado canal de IRC. Los bot están conectados permanentemente al canal y cuando hay un comando lo reciben y lo ejecutan.

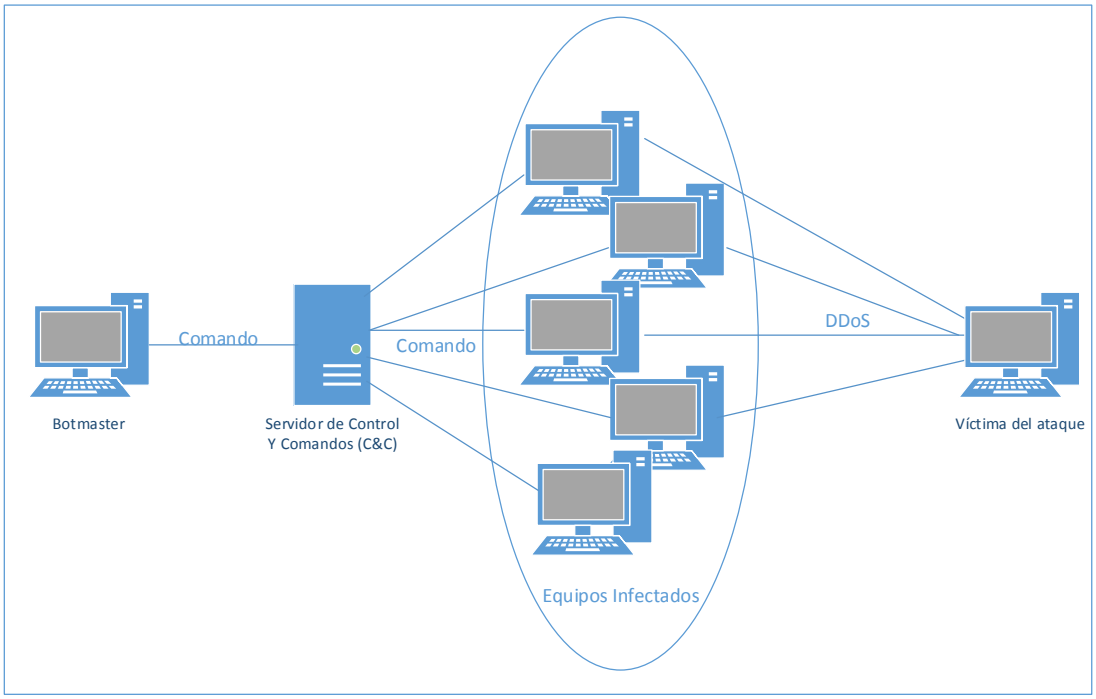

Figura 35. Arquitectura de una botnet

Este tipo de botnets se consideran débiles, ya que tienen un punto débil en el servidor de control y comandos (C&C), ya sea una página web o un canal de IRC. Por ello las nuevas botnet siguen una arquitectura más compleja, son las llamadas botnets p2p.

Estas redes p2p son más resistentes, este tipo de arquitectura completamente descentralizado hacen que sean más robustas, en este tipo de redes cada equipo infectado es a su vez atacante directo y servidor de comandos. Para el envío de información se utiliza el protocolo P2P, el botmaster puede elegir entre cualquiera de los protocolos P2P existentes. Suele haber dos

niveles de equipos infectados (zombies), los que tienen capacidad de reenviar los comandos y los que no.

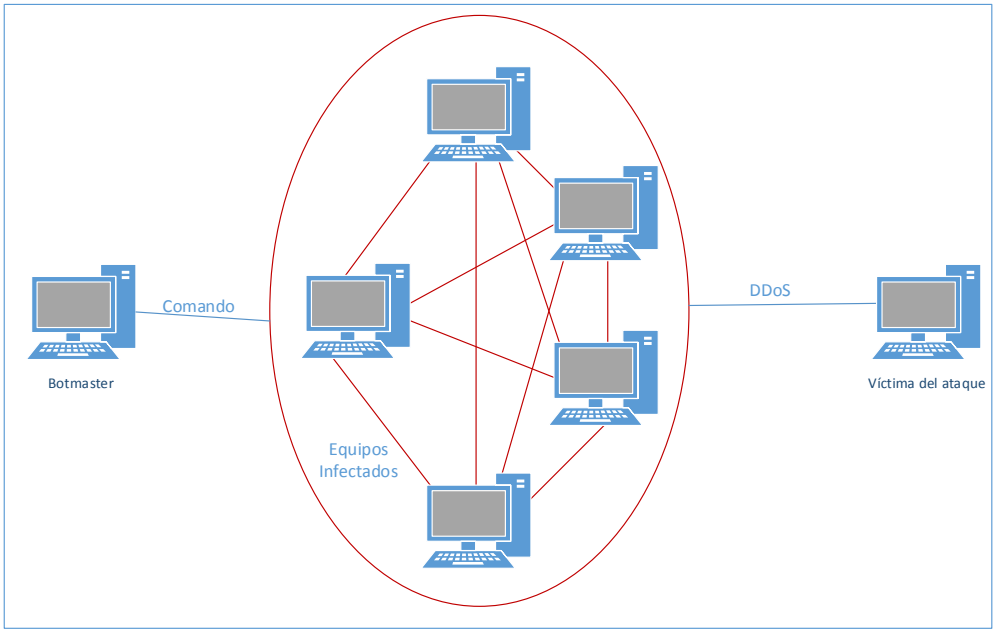

Figura 36. Arquitectura de Botnet P2P

5.3.2. Tipos de ataque DDoS:

Vamos a hacer una división en función de a que actor de la red afecta el ataque, contra la red, contra los servidores o contra la aplicación.

Ataques contra los recursos de red:

Este tipo de ataques buscan consumir todo el ancho de nada con tráfico ilegítimo para saturar un canal determinado. Un cliente legítimo se encontrará con servicios no disponibles o extremadamente lentos.

UDP Flood (inundación UDP): UDP es un protocolo no orientado a la conexión, que usa datagramas sobre IP. Un ataque de inundación UDP no explota una vulnerabilidad específica, el ataque básicamente usará una red para enviar gran número de paquetes a puertos aleatorios, normalmente apoyado sobre IP spoofing. El servidor que recibe la petición no es capaz de procesar cada petición y consume todo su ancho de banda enviando ICMP "destination unreachable" indicando que la aplicación no está disponible para escuchar en el puerto solicitado.

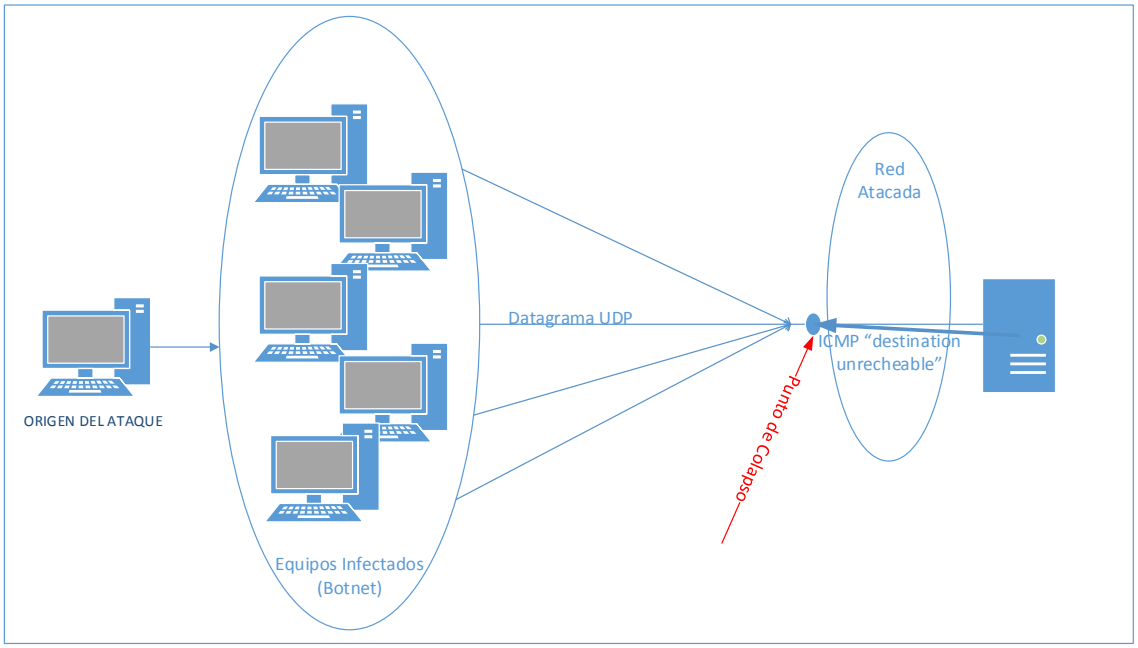

Figura 37. Ataque UDP Flood

ICMP Flood: ICMP es usado para operaciones IP, diagnósticos y errores. Al igual que el ataque UDP Flood no aprovecha una vulnerabilidad concreta, su funcionamiento consiste en enviar mensajes Echo request y que los mensajes Echo Reply sean los que inunden la red atacada. Si en la red atacada hay un gran número de equipos en el mismo segmento de red se puede producir una amplificación del efecto. Cuando se produce esta amplificación por un envío ICMP a la dirección de broadcast de la red atacada se denomina ataque **Smurf**, actualmente la mayoría de los sistemas están preparados para no reenviar este tipo de mensajes[40].

IGMP Flood: IGMP también es un protocolo sin conexión usado por equipos IP, como servidores y routers. Tampoco depende de ninguna vulnerabilidad. Su funcionamiento es sencillo, simplemente enviar reportes IGMP a una red o router, esto hace que el tráfico a través de un determinado router se ralentice y el tráfico legítimo se ve penalizado.

Ataques contra los recursos del servidor:

En estos ataques se busca colapsar los recursos de un servidor, normalmente la capacidad de procesamiento o la cantidad de memoria, causando una denegación de servicio. La idea es que el atacante puede a través de una vulnerabilidad en el equipo atacado o un punto débil en el protocolo de comunicación. Los servidores que normalmente son atacados son los que

[40] En routers Cisco se utiliza el comando *no ip directed-broadcast*

albergan aplicaciones web o páginas web. Aunque este tipo de ataques muchas veces afectan al rendimiento de otros sistemas como firewalls o IPS e IDS.

Este tipo de ataques se aprovechan de los puntos débiles del protocolo TCP/IP, estos puntos débiles son la falta de uso de los 6 bits de control del protocolo TCP/IP (Flags: SYN, ACK, RST, PSH, FIN y URG). TCP/IP es un protocolo basado en la conexión por lo que se debe establecer previamente la conexión antes de cualquier envío. TCP/IP depende de un mecanismo de negociación en tres pasos, cada conexión crea la mitad de la conexión (SYN), una petición de respuesta (SYN-ACK) y una confirmación (ACK). Los ataques intentan abusar de estas debilidades básicamente enviando paquetes TCP en desorden, consiguiendo colapsar el servidor intentando procesar los paquetes erróneos.

TCP SYN Flood: el atacante (cliente) hace creer al servidor que está recibiendo una petición legítima a través de una serie de peticiones con el flag SYN activado, con IP suplantadas (spoofing). Para contestar a estas peticiones el servidor abrirá un hilo para cada petición y reservará el espacio para los buffer. Cuando envíe el correspondiente SYN-ACK de respuesta al tratarse de direcciones IP no válidas o servidores preparados para no responder nunca recibirá el correspondiente ACK de confirmación de la conexión. El servidor seguirá reservando espacio y reenviando los paquetes SYN-ACK hasta que se produzca un time-out. Si el servidor recibe muchas de estas conexiones acabará produciéndose una denegación de servicio.

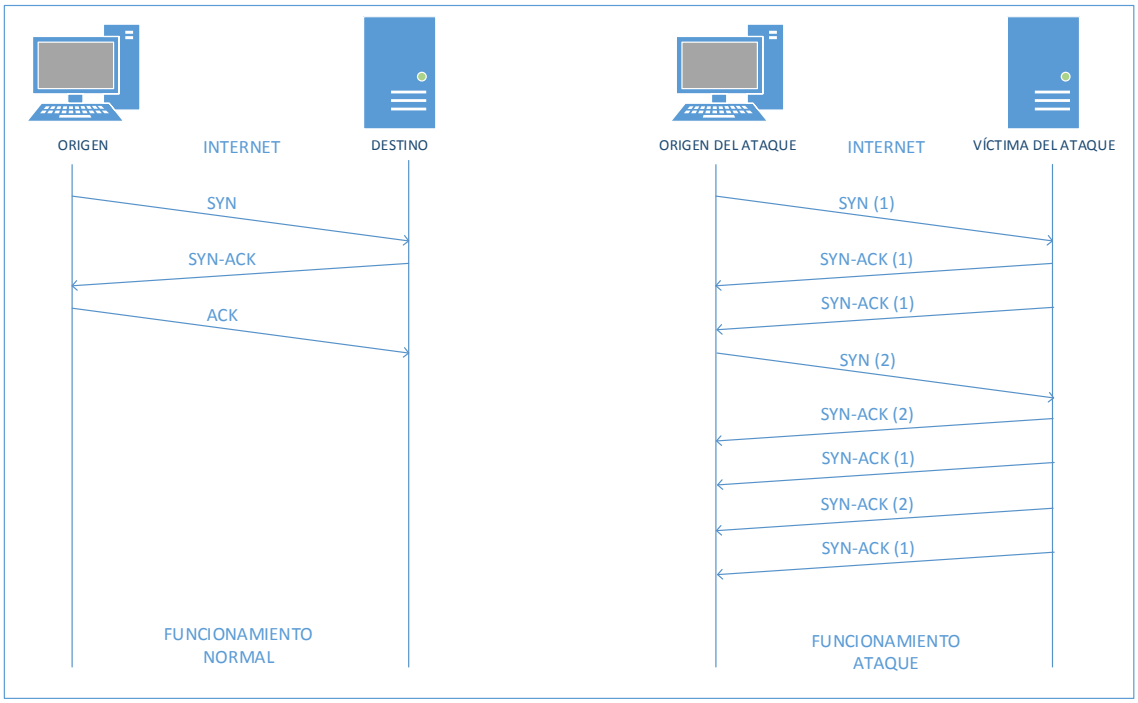

Figura 38. Comportamiento normal TCP y comportamiento ante un ataque TCP SYN Flood

TCP RST Attack: en condiciones normales de una conexión TCP el bit RST está a 0, sin embargo si hay un problema en la conexión el bit estará a 1, lo que indica a las dos partes que se debe interrumpir automáticamente la conexión TCP. Esto permite a un tercero enviar paquetes TCP con el bit a 1 a ambos extremos de la conexión.

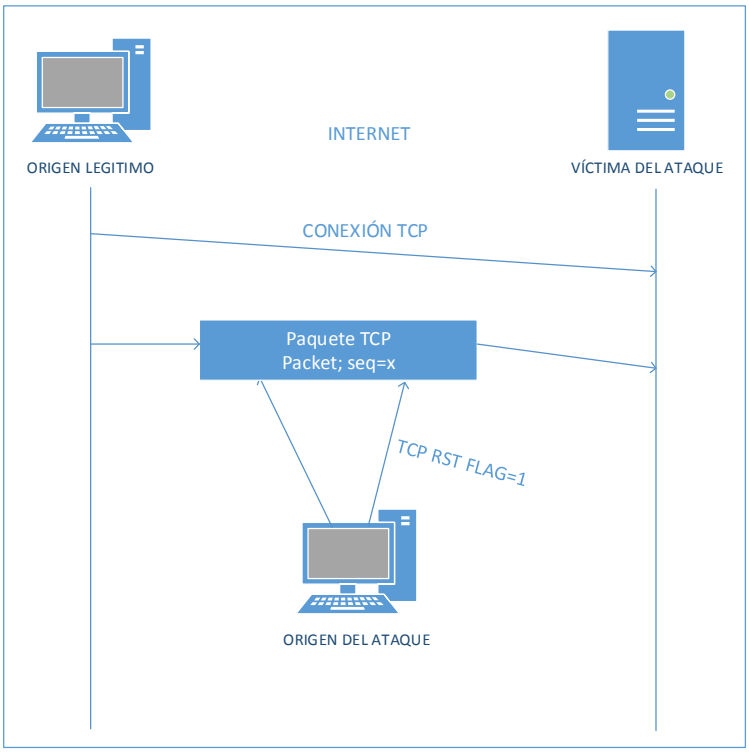

Figura 39. Ataque RST.

TCP PSH + ACK Flood: cuando se envía un paquete TCP con el flag PSH a 1, el resultado es que los datos TCP son enviados directamente al receptor, que es forzado a limpiar su buffer y enviar una confirmación de recepción. Un atacante a través de una botnet puede inundar un servidor con muchas peticiones llegando a un punto de denegación del servicio cuando el servidor no es capaz de responder todas las peticiones.

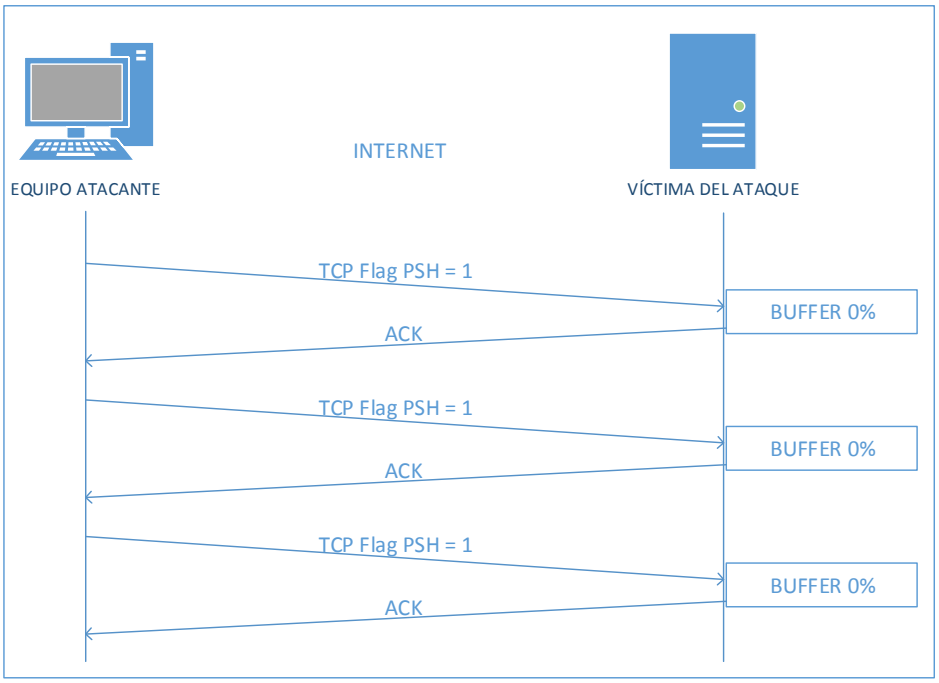

Figura 40. Ataque TCP PSH + ACK FLood

No todos los ataques son por inundación, también están los conocidos como ataques **Low and Slow,** estos ataques requieren menos cantidad de tráfico para ser efectivos, se basan generalmente en vulnerabilidades de los sistemas. Al no requerir gran cantidad de tráfico son más difícil de detectar.

Sockstress: es un ataque *low and slow*. Como ya hemos comentado, en el proceso de negociación TCP necesitamos un SYN, un SYN-ACK y un ACK, en el momento que llega el ACk se ha establecido la conexión. Los atacantes en este tipo de ataque establecen correctamente la conexión TCP pero envían paquetes con tamaño de ventana 0 (window size 0) en el último ACK. De esta forma configuran el buffer que reserva la conexión a 0 bytes. De esta forma la conexión está siempre abierta, el sistema atacado generará paquetes PROBE[41] para preguntar por el tamaño de la ventana. Si el atacante genera varias conexiones de este tipo, conseguirá que la tabla de conexiones de TCP se llene y no se puedan recibir peticiones legítimas.

Otra variante de este ataque es configurar la ventana a un tamaño muy pequeño, añadiendo a la problemática el hecho de tener que estar dividiendo la información en pequeñas fracciones llegando también a forzar una denegación de servicio.

[41] Los paquetes *probe* se utilizan en conexiones sin dato. El número de secuencia y el de confirmación están a 0.

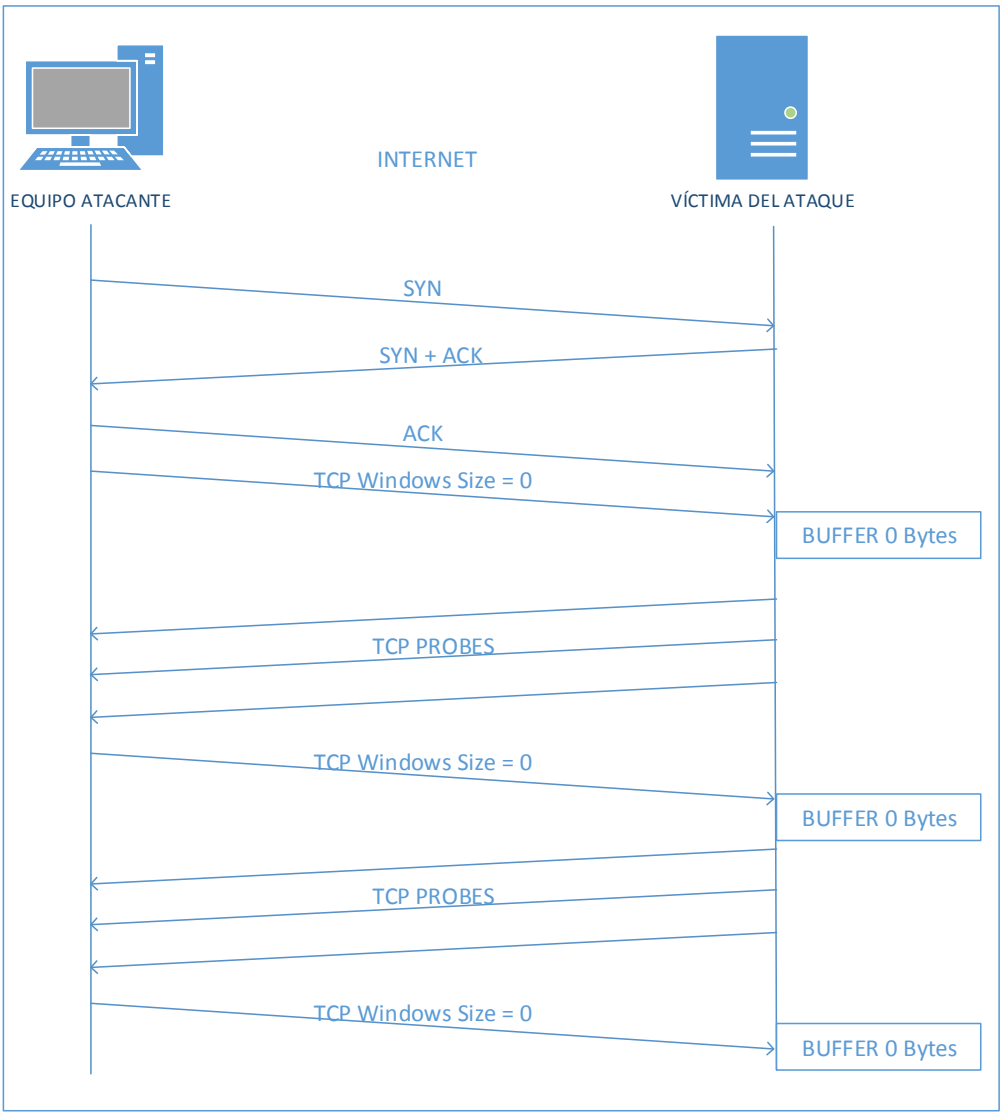

Figura 41. Ataque Sockstress

Con el aumento de los servicios que usan SSL como método de encriptación SSL, los atacantes han encontrado un nuevo objetivo para los ataques SSL. Los ataques basados en ssl son de dos tipos, los que atacan el mecanismo de establecimiento de la conexión, mandando basura al servidor ssl o atacando el proceso de intercambio de claves. La encriptación supone un problema a la hora de detectar un ataque ya que los mecanismos de detección no son capaces de examinar el tráfico.

HTTPS Floods: es un ataque basado en SSL. Casi todo el negocio en Internet usa encriptado SSL/TLS para securizar el tráfico extremo a extremo de sus aplicaciones. Un ataque https flood es un ataque http flood (ver detalle en el apartado siguiente) que es mucho más difícil de detectar, porque, como ya hemos comentado las utilidades preparadas para examinar el tráfico y detectar este tipo de ataques no desencriptan el tráfico.

THC-SSL-DOS: Este tipo de ataques requiere un pequeño número de paquetes para causar una denegación de servicio. El ataque comienza con una negociación estándar SSL, que inmediatamente solicita la renegociación de las claves de encriptación, pidiendo constantemente esta renegociación se consigue que el servidor no sea capaz de responder todas las peticiones. Este tipo de ataque es muy efectivo por el coste de recursos en el atacante es mucho menor que en el atacado (del orden de 15 veces superior).

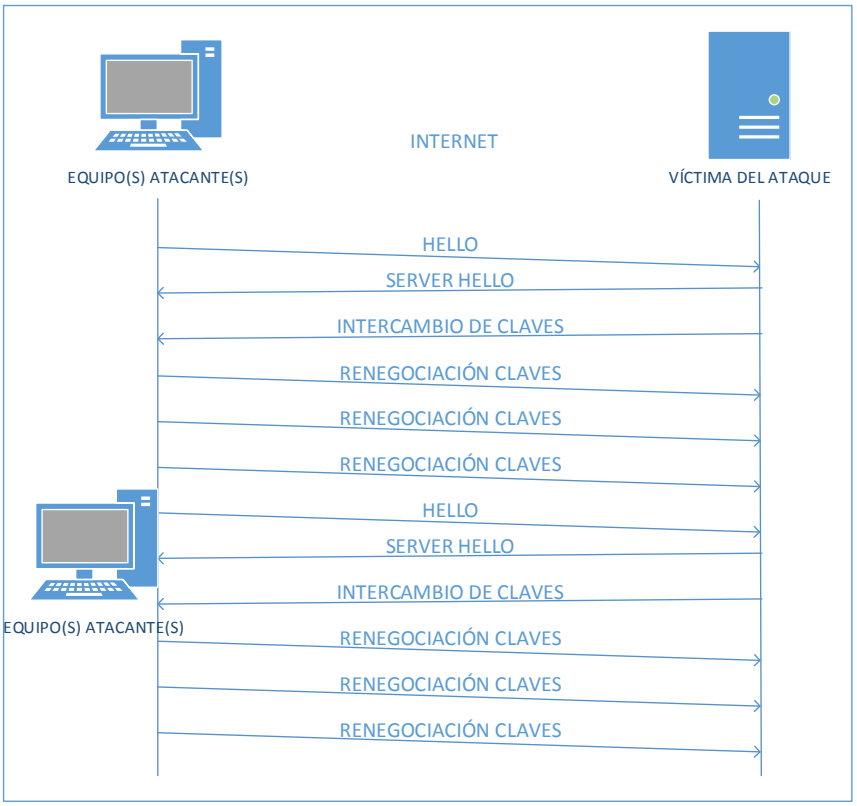

Figura 42. Ataque THC SSL DDoS

Ataques contra los recursos de aplicación:

Los ataques contra los recursos de aplicación son cada vez más usados, cada servicio de Internet tiene sus debilidades.

HTTP Flood: es el más común de los ataques DDoS contra los recursos de aplicación. Es un ataque a nivel 7 del modelo OSI, utiliza peticiones estándar GET y POST. Son ataques por volumen, no se usan IP suplantadas ni paquetes malformados. Normalmente intentan hacer peticiones complejas, como peticiones a bases de datos para que sobrecargue más el servidor. Normalmente se utilizan botnets para hacer el ataque efectivo.

DNS Flood: una ataque de inundación de DNS es fácil de hacer y muy difícil de detectar. Es una variante de UDP Flood, ya que DNS usa los servicios de UDP para funcionar. Este tipo de ataque simplemente envía millones de peticiones DNS a un servidor haciendo que se produzca una denegación de servicio.

Al igual que hablábamos de ataques a servidores **Low and Slow**, contra las aplicaciones también se producen este tipo de ataques. Estos ataques buscan aprovechar las vulnerabilidades de las aplicaciones. No son ataques por volumen, normalmente ocurren en la capa de aplicación cuando el enlace TCP ya está establecido, haciendo que el tráfico malicioso se mezcle y pase por tráfico legítimo.

Slow HTTP GET Request: la idea de este tipo de ataques es hacerse con la mayoría de los recursos de la aplicación haciendo uso de demasiadas conexiones. Es este ataque se envían peticiones HTTP GET completas al servidor, que abre un hilo para cada una de estas peticiones y espera a que el resto de la información se envíe, el atacante continúa enviando cabeceras HTTP para que el enlace no se cierre por un timeout. Como los datos llegan muy despacio las conexiones permanecen abiertas y llenan las tabas de conexiones llegando a producir una denegación de servicio.

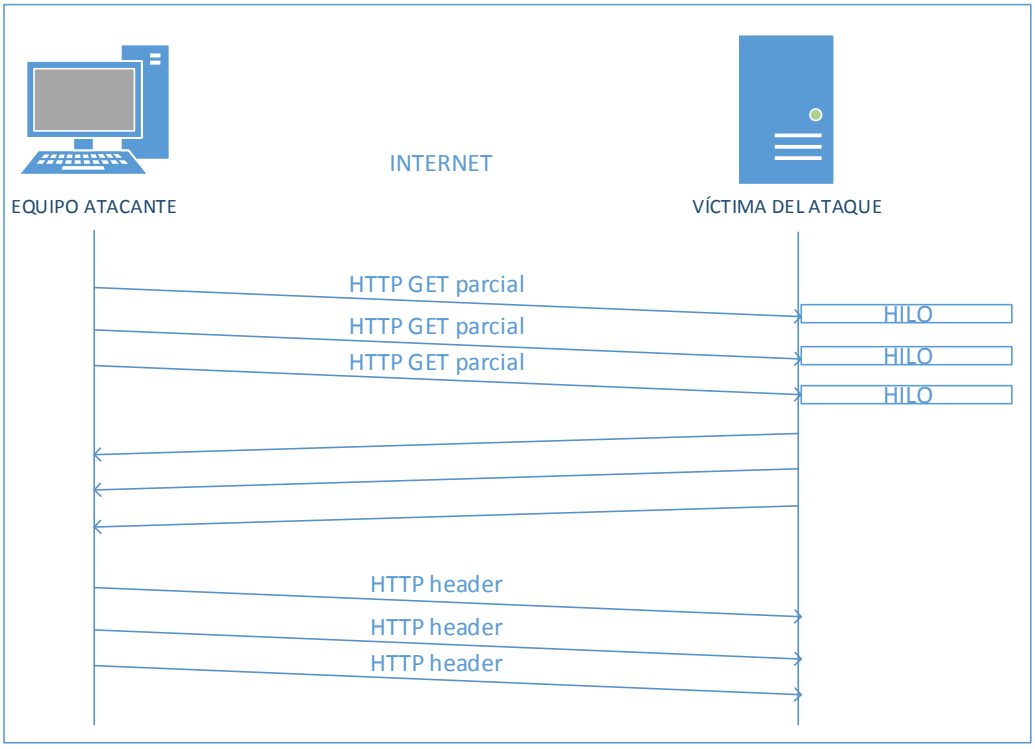

Figura 43. Ataque Slow http get request

Slow HTTP POST Request: el atacante busca los formularios disponibles en una página web y envía peticiones HTTP POST a través de esos formularios, las peticiones post son enviadas byte a byte, este envío se hace de forma lenta pero de manera que se mantenga la conexión activa, enviando cada byte en función de los timeout que cerrarían la conexión. Este tipo de funcionamiento es válido porque se mantiene para usuarios legítimos con conexiones lentas. El atacante repite esta operación cientos de veces hasta conseguir la denegación de servicio no permitiendo a los usuarios legítimos acceder a la aplicación.

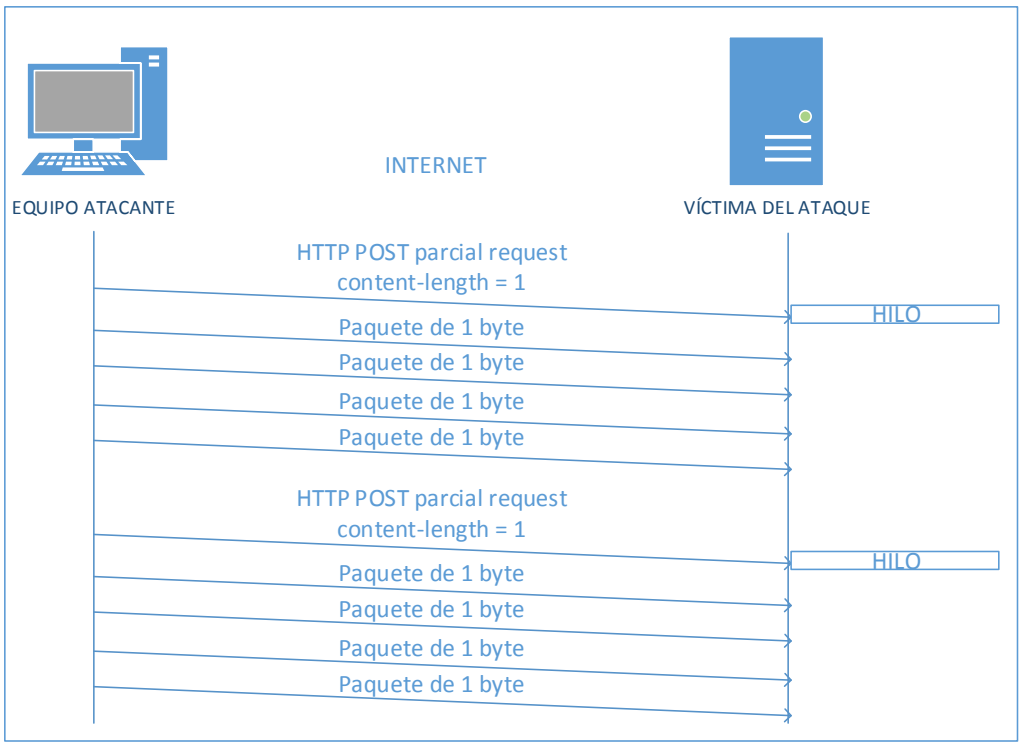

Figura 44. Ataque Slow HTTP Post Request

Regular Expression DOS Attack (ReDoS): es un ataque *low and slow* en el que el atacante envía un mensaje especialmente creado llamado *evil RegExes* que utiliza una vulnerabilidad en las librerías del servidor, concretamente en las librerías de las expresiones regulares. Esto causa que el servidor consuma gran cantidad de recursos mientras trata de procesar la expresión regular.

Hash Collisions DoS Attack: muchos servidores de aplicación crean una tabla con sumas de verificación para indexar los parámetros de las sesiones POST. En ocasiones si se produce una colisión hash hay que procesarla. Este tipo de procesamiento requiere gran cantidad uso de CPU, el ataque se produce para usar esta debilidad de funcionamiento, el atacante envía un mensaje POST con gran cantidad de parámetros preparados para causar colisiones hash en el

lado del servidor. Esto puede llegar a causar denegación de servicio al llegar a cargas muy altas de la máquina.

5.3.3. Herramientas para ataques DDoS

Hay multitud de herramientas para realizar ataque de denegación de servicio, algunas de ellas son o naces como herramientas para comprobar la capacidad de un servidor, o comprobar un desarrollo. A continuación detallo algunas de las más usadas y accesibles:

LOIC (Low Orbit Ion Cannon): creada en origen para hacer pruebas de carga de servidores web por los propios programadores y analistas de sistemas. Es una simple herramienta de inundación, preparada para generar un gran número de tráfico TCP, UDP o HTTP.

El grupo de activistas Anonymous comenzó a usar este software para hacer ataques DDoS.

Desde la versión 1.1.1.3 se añade la funcionalidad de que la aplicación sea controlada por el operador de un canal de IRC. Para evitar saber el origen de estos ataques se suelen usar a través de las redes oscuras[42].

Como vemos en la captura de pantalla, hacer un ataque DoS es extremadamente sencillo.

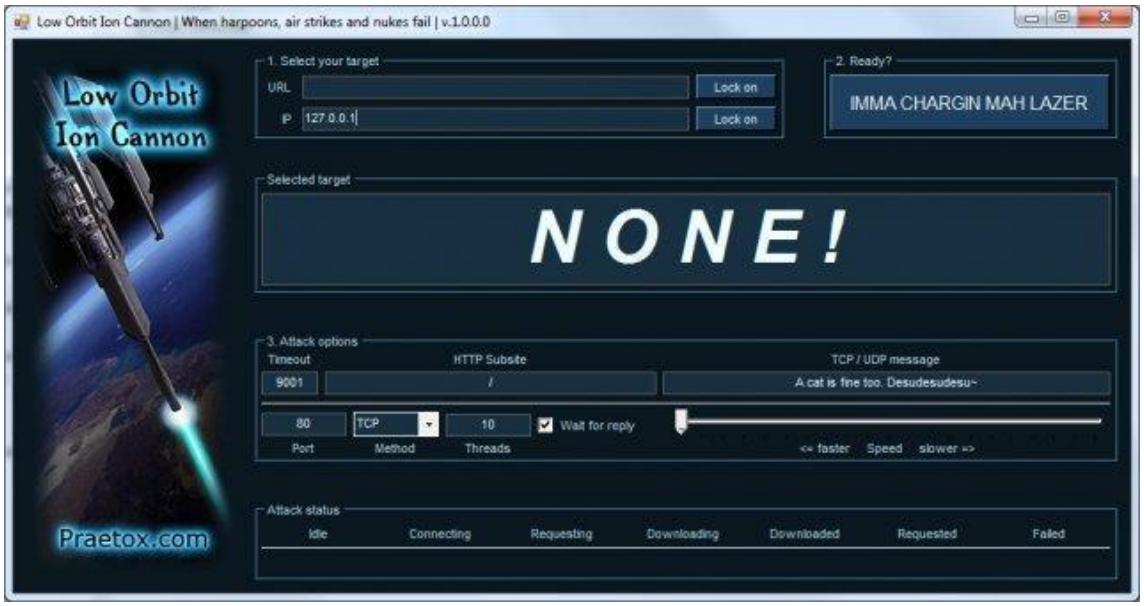

Figura 45. Captura de pantalla de LOIC. Fuente: Github de LOIC. (28)

(28) **LOIC.** Github de LOIC. *Github.* [En línea] http://sourceforge.net/projects/loic/.

[42] Ver punto 4

HOIC (High Orbit Ion Cannon): es una sencilla aplicación para el envío de HTTP POST y HTTP GET con una interfaz gráfica de usuario muy sencilla. Se le pueden añadir addons para modificar los ataques. HOIC no permite el control remoto como LOIC, ni tampoco utiliza ningún medio de ocultación del origen del ataque. Anonymous lo ha usado como sustituto de LOIC porque es más difícil de localizar.

En este caso las IP a atacar se insertan en un fichero de configuración.

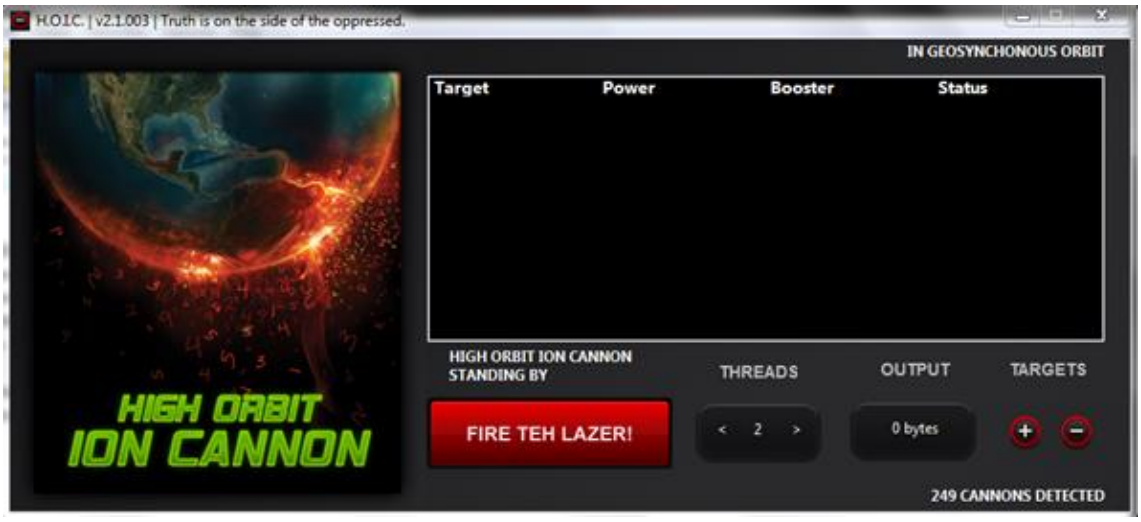

Figura 46. Captura de Pantalla de HOIC. Fuente: skynetcyber4rt.blogspot.com.es (29)

HPING: es un software de línea de comandos con una funcionalidad similar a la del comando ping, además de la funcionalidad típica del comando ping este software permite generar gran volumen de tráfico TCP. Soporta los protocolos TCP, UDP, ICMP y RAW-IP. Tiene la capacidad de suplantar IPs.

Slowloris: es un script perl que implementa una herramienta para generar ataques DDoS contra servidores apache. Su funcionamiento consiste en saturar el pool de servicios mediante un ataque slow HTTP/S request.

R.U.D.Y. (R U Dead Yet?): de nuevo nos encontramos ante una herramienta para hacer ataques slow HTTP/S request.

#Refref: desarrollado directamente con Anonymous, se basa en aprovechar vulnerabilidades de SQL. Mediante inyección de código SQL, es capaz de enviar querys SQL malformadas. Con muy pocos equipos son capaces de realizar un ataque con muy pocos recursos. Se puede usar en cualquier equipo con soporte javascript.

(29) **amiri, Novan.** Skynet Cyber4RT. *Software HOIC.* [En línea] http://skynetcyber4rt.blogspot.com.es/2014/06/blog-post_182.html.

5.3.4. Ataques DDoS más importantes

Se calcula que se producen del orden de 2000 ataques de denegación de servicio diarios (30), a continuación podemos ver ejemplos de los que más impacto han tenido:

Ataque de Mafiaboy contra Yahoo, Ebay, Amazon, ZDNet: se considera el primer gran ataque de denegación de servicio, fue en febrero de 2000 y un hacker de 15 años atacó las principales web mundiales, paralizándolas durante horas. Sólo Yahoo estimó sus pérdidas en 500.000 dólares. Mafiaboy, que por aquel entonces sólo tenía 15 años, comprometió una serie de servidores gracias a una vulnerabilidad conocida, aprovechando esta vulnerabilidad para instalar un software para convertirlos en equipos de una botnet. Los equipos infectados eran capaces de atacar e infectar otros sistemas.

El culpable fue detenido en Canadá y condenado a 8 meses en un centro de menores.

Operación Payback: el grupo de activistas Anonymous sale en defensa de Wikileaks dirigiendo un ataque DDoS con las compañías que habían tomado acciones contra Wikileaks, Amazon, Paypal, Master Card o Visa se vieron afectadas. Las páginas de estas dos últimas estuvieron fuera de servicio el 8 de diciembre de 2010. Este se considera el primer ataque en superar la barrera de los 100Gbps. Para realizar este ataque se utilizó la herramienta LOIC[43].

Operación Chanology (Anonymous contra la iglesia de cienciología): en febrero de 2008 Anonymous ataca la web scientology.org, llegándola a hacer inaccesible con un ataque considerado medio, con un poco de 200Mbps, y una carga media en la inundación de 168Mbps La web llegó a estar inaccesible.

Ataque a Spamhaus: Spamhaus es una empresa líder en servicios antispam. El 18 de marzo de 2013 sufrió el que se considera el ataque DDoS más importante de la historia. El ataque empezó recibiendo aproximadamente 10Gb/s de peticiones, pero fue aumentando a medida que se intentaban mitigar los daños. En el momento más importante del ataque se llegó a recibir 300Gb/s, llegando a afectar a los niveles Tier[44] 1 y 2 de Internet.

(30) **map, digitalk attack.** Digital Attack Map. *Undertanding DDoS.* [En línea] http://www.digitalattackmap.com/understanding-ddos/.

[43] Ver punto 5.3.3

[44] Una red Tier 1 es el nivel más alto de Internet si vemos esta como una red jerárquica, sólo hay un limitado número de ISP en este nivel, tienen cobertura internacional. Las redes Tier 2 se conectan directamente a las Tier 1 y forman el segundo nivel jerárquico. Tienen cobertura nacional.

En un momento del ataque se empezaron a atacar los puntos neutros[45] de Internet, consiguiendo colapsar el punto neutro situado en Londres por lo que se vio afectada la navegación en toda esta zona.

El ataque aprovechó el funcionamiento de los DNS, utilizando IP spoofing, se realizó un ataque de tipo smurf, los equipos atacantes hacen millones de peticiones DNS a los servidores DNS, pero modifican la IP origen de la petición, por lo que las respuestas llegan a la IP atacada. Se estima que llegaron peticiones de más de 30000 servidores DNS distintos. (31)

Un mes después del ataque se detuvo a una persona como responsable del ataque, ataque que fue revindicado por un grupo llamado Cyberpunk. (32)

Aiplex contra Anonymous: en 2010 Aiplex Software, una compañía de software India fue contratada por los estudios de grabación para atacar las páginas con contenido con copyright, debido a este intento de ataque Anonymous atacó la web de Airplex y la RIAA y la MPAA. Dejando sin servicio las webs de estas.

5.3.5. Como detectar y defenderse de un ataque DDoS

Las soluciones clásicas de seguridad no funcionan para mitigar un ataque de denegación de servicio, normalmente las empresas basan su seguridad en un firewall más o menos avanzado, pero normalmente estos no llegan a los niveles de aplicación, normalmente se limitan a analizar unos pocos bytes para minimizar la latencia. Normalmente los ataques utilizan puertos y servicios que necesitamos tener abiertos para el funcionamiento normal de nuestras aplicaciones.

En redes más avanzadas vemos IDS/IPS implementados, que son incluso capaces de detectar un ataque DDoS, pero en la mayoría de los casos no son capaces de mitigar el ataque.

(31) **securitybydefault.** securitybydefault. *Cómo CyberBunker atacó a Spamhaus y casi se llevó a medio Internet por delante.* [En línea] http://www.securitybydefault.com/2013/03

/como-cyberbunker-ataco-spamhaus-y-casi.html.

(32) **Romero, P.** elmundo.es. *El detenido por el 'ciberataque' a Spamhaus dice ser 'diplomático de la Rep. de Cyberbunker'.* [En línea]
http://www.elmundo.es/elmundo/2013/04/28/navegante/1367139728.html.

[45] Un punto neutro (IXP) es el punto de acceso físico a través del cual se conectan los proveedores de internet a Internet.

Aunque normalmente los efectos de un ataque los podemos detectar por el rendimiento de la máquina o de la red, es conveniente intentar detectar antes los ataques, a continuación vemos algunas formas de detección:

Analizador de protocolos: usando un analizador de tráfico como whireshark, para observar el tráfico y ver que está pasando, además podemos ver que ha pasado con posterioridad si lo tenemos capturando el tráfico. Por desgracia este tipo de detección es manual, requieren de un operador que analice lo que está pasando.

Software de monitorización: aunque no nos van a avisar de un ataque de DDoS, este tipo de software (como puede ser Nagios) si nos va a avisar de un mal funcionamiento en nuestros sistemas. Desde un uso de ancho de banda excesivo a una caída de un servicio como puede ser un servidor web puede ser la pista para saber que estamos siendo atacados. Esto nos podrá anticiparnos en muchos casos al colapso de nuestros servicios, aunque en muchos casos cuando se produce el aviso ya nos encontramos en un estado muy avanzado del ataque.

A continuación vemos algunos de los métodos usados para defenderse de un ataque:

Overprovisioning (exceso de ancho de banda): Algunas empresas, especialmente ISP y proveedores de servicios en la nube utilizan lo que se conoce como exceso de aprovisionamiento, es decir, disponen de anchos de banda totalmente desproporcionados que, en teoría serían capaces de tener ancho de banda suficiente en caso de un ataque. Además de tener ancho de banda suficiente debemos asegurarnos que el servidor o clúster de servidores es capaz de procesar todo este tráfico sin verse bloqueado. Este tipo de defensa se considera poco efectiva en función del coste necesario, además, no es efectiva contra los ataques DDoS contra los recursos de aplicación.

Clean-pipe: es una solución que ofrecen los ISP, es el propio ISP el que monitoriza e inspecciona el tráfico y encamina el tráfico sospechoso a un proxy que limpia el tráfico. Este tipo de herramientas pueden ser efectivas, pero requieren que el ISP disponga de toda la información referente a tu tráfico. Uno de los problemas de este tipo de servicios es que puedes verte afectado por un ataque a alguien que utilice los servicios del mismo ISP, el otro gran problema es que se puede perder tráfico legítimo. Este tipo de defensa es reactivo, es decir, cuando ya se ha producido el ataque. No se considera muy efectivo cuando el ataque es muy potente (gran número de atacantes) o hay gran número de víctimas.

Proveedores especializados: hay proveedores especializados en este tipo de ataques. Además de ser capaces de absorber el tráfico necesario, realizan análisis forenses de los ataques y mitigan el ataque.

5.4. Sistemas antivirus

El software malicioso existe hace muchos años, el primer virus informático conocido como tal está datado en 1972 y es conocido como Creeper, este primer virus fue también el origen del primer software antivirus, Reaper. Aunque podía ser destructivo, el software malicioso[46] no ha sido de verdad una preocupación hasta que los equipos han estado conectados a Internet. Hasta hace poco eran exclusivos de los equipos con arquitectura para ordenadores personales o servidores, pero en los últimos años ha salido del mundo de los pc y servidores para llegar a los terminales móviles inteligentes (móviles, tabletas, relojes…). Todo esto, como ya vimos en el apartado 3.3, hace que las posibles víctimas se multipliquen.

El objeto de este tipo de software depende del tipo de software malicioso que veremos a continuación, pero de una forma general podemos decir que el software malicioso:

- Robo de información
- Destrucción de la información
- Publicidad no deseada
- Fraude/Estafa al usuario
- Uso del equipo de manera remota

A continuación vamos a ver los tipos de software malicioso:

Software de publicidad no deseada (Adware): este tipo de malware está pensado para mostrar publicidad a los usuarios sin el consentimiento de este. No todo el software que muestra publicidad es considerado software malicioso, sólo el que la muestra sin que el usuario lo haya elegido, o si lo hace de forma molesta o en situaciones que interfieren en el software legítimo del usuario. En este tipo de software malicioso se incluyen las barras que se

[46] En inglés y por tanto de uso común en la red, se usa el término Malware para referirse al software malicioso.

añaden a los navegadores de forma no deseada o el cuándo se fuerza la página de inicio o el buscador de un navegador.

Software espía (Spyware): usado para recopilar información del usuario, que posteriormente será envida a un tercero sin el consentimiento del usuario. El uso de estos datos puede ser muy variado, desde tobo de datos bancarios, extorsión, a simplemente ser usados para mostrar publicidad no deseada al usuario, formando parte de un adware.

Aparte del robo de datos, este tipo de software afecta a la estabilidad y rendimiento del equipo infectado, ya que se están ejecutando continuamente.

Redes Zombi (Botnets): Una red zombie es un conjunto de equipos interconectados, estos equipos están infectados y pueden ser controlados de forma remota. Un equipo que integrado en una red zombi podrá ser utilizado por los delincuentes para distintos delitos, lo más típico es unir fuerzas para un ataque de denegación de servicio o utilizar el equipo infectado para el envío de SPAM. Desde el año 2011 se ha reportado una nueva funcionalidad, esta es la minería de la moneda virtual Bitcoin[47].

Troyanos: un troyano es un software pensado para controlar el equipo infectado, normalmente el nivel de acceso obtenido por el troyano es el mismo que el del usuario que ha ejecutado el software en el que venía oculto el troyano. Las acciones típicas que ejecutan los delincuentes tras este tipo de software malicioso son agregar la máquina a una botnet, instalación de otros software, eliminación o modificación de ficheros, robo de información (a través de keyloggers, capturas de pantalla, etc.). Con la llegada a los terminales móviles, se ha añadido nueva funcionalidad a este tipo de software, como puede ser el realizar una llamada, o leer los SMS de un usuario.

Gusanos (IWorm): aunque de percepción similar a otros tipos, los gusanos simplemente se limitan a clonarse a sí mismos, a diferencia de otro tipo de software malicioso, no necesitan modificar otro tipo de ficheros, pueden incluso residir en memoria. Simplemente replicándose y reenviándose son capaces de llegar a colapsar redes enteras y con mucha facilidad a impedir el funcionamiento normal del equipo infectado, sobre todo, las tareas de red.

Scareware: este tipo de software se aprovecha del miedo y desconocimiento del usuario, en ocasiones sólo para asustarle, pero en la mayoría de los casos la motivación es cometer una

[47] Bitcoin es la primera “criptodivisa” creada. Es una divisa descentralizada apoyada en una red p2p, los bitcoin se generan a través del proceso llamado minería. Actualmente hay otras “criptodivisas”, pero ninguna con la aceptación y uso de bitcoin.

estafa económica. La mayoría de este tipo de software tiene un funcionamiento muy sencillo: un aviso en el equipo infectado alerta al usuario que ha sido infectado por un virus y le sugiere pagar un software antivirus para solucionarlo, este software por el que pagan en la mayoría de los casos ni existe ni elimina el aviso.

Keyloggers: como su propio nombre indica un keylogger se encarga de registrar las pulsaciones de las teclas del equipo infectado, la información recogida se envía a un tercero para cometer un acto delictivo. En la mayoría de los casos se utiliza para el robo de contraseñas, ya sean bancarias o de acceso a servicios.

RootKits: es un software de acceso al equipo infectado, llega a niveles de sofisticación tales que su presencia es prácticamente imperceptible, ya que se oculta al control del usuario. Normalmente son capaces de modificar los sistemas encargados de detectarlos. Su funcionamiento consiste en la instalación de puertas traseras para acceder al equipo infectado, ocultar lo que se ha modificado y modificar los registros para evitar que sea detectado.

Puertas Traseras (Backdoor): una puerta trasera es un fallo dentro de un código legítimo, normalmente puesta a propósito por el programador, mediante estos fallos de programación se puede acceder al sistema infectado.

Cadenas de mensajes: Aunque no es un software malicioso como tal, en muchos casos se han utilizado las cadenas de correos para recopilar datos personales, especialmente direcciones de correo electrónico que posteriormente se utilizarán para el envío de publicidad no deseada. En muchos casos este tipo de cadenas también incluye algún tipo de enlace a otros tipos de software malicioso o a alguna página web.

Quizás el caso más famoso de un virus informático es el caso del gusano Blaster, que en 2003 hizo estragos en los ordenadores de medio mundo, su funcionamiento era sencillo, simplemente provocaba el desbordamiento del buffer del servicio DCOM en equipos Windows, en el momento que se produce un desbordamiento de este buffer el equipo inicia el procediendo de apagado por lo que dejaba el equipo inutilizable. Su autor, de origen estadounidense fue sentenciado a 18 meses de prisión.

A raíz de todo este tipo de software malicioso, surge el software para combatirlo.

5.4.1. Cómo combatir el malware

Los comúnmente conocidos como sistemas antivirus nacen de la necesidad de combatir el malware en todas sus vertientes, se tratan de programas creados para erradicar los virus informáticos.

A continuación vamos a detallar las funcionalidades que pueden tener los sistemas anti-malware. No todos disponen de todos los tipos de defensa:

Análisis en tiempo real: es lo mínimo que le podemos pedir a un software antimalware que instalemos en un ordenador para tener una protección continuada. Analiza los ficheros cuando son accedidos, es decir si un fichero no es accedido el antivirus no será capaz de detectarlo.

Análisis de la memoria del sistema: normalmente son parte de los análisis en tiempo real, buscan virus en la memoria del sistema en tiempo de ejecución.

Análisis completo del sistema: este tipo de análisis es forzado por el usuario, sirve para buscar ficheros que no han sido accedidos por lo tanto no han podido ser detectados por el monitor de virus en tiempo real.

Protección del correo electrónico: el antivirus es capaz de analizar el correo electrónico según se descarga el gestor de correo electrónico (como Microsoft Outlook o Mozilla Thunderbird), de esta manera los virus son detectados antes de que puedan ser accedidos por el usuario y por tanto evitan la infección del equipo.

Protección anti--spyware: buscan software con el comportamiento típico de los spyware. En muchos casos aunque el software sea capaz de detectar el spyware no es capaz de eliminarlo y son necesarios procedimientos específicos para cada tipo de spyware.

Protección anti-adware: buscan malware de este tipo, que normalmente no es detectado por los antivirus convencionales, hay antivirus que tienen este tipo de módulos, aunque también hay software anti-adware específico.

Ejecución aislada (sandbox): es una funcionalidad relativamente reciente, nos da la oportunidad de ejecutar un software en un entorno controlado. Por lo que si se trata de un software malicioso no podrá acceder a partes críticas del sistema. Una vez que el software es ejecutado en el entorno protegido, se comprueba que el software no acceda a partes del sistema que no debe acceder o intente modificar alguna parte del sistema que está

monitorizada. En caso de que se produzcan este tipo de comportamiento el entorno destruirá los cambios en el momento que se termine la ejecución

El problema de este tipo de ejecución es que en muchas ocasiones este tipo de ejecución hace que el software legítimo no funcione correctamente.

Análisis de direcciones web: al igual que en la detección de virus clásica basada en bases de datos hay anti malware que posee una serie de direcciones que han dado positivo a software malicioso, de esta forma es capaz de avisar antes del acceso a este tipo de web.

Software antispam: buscan emails no deseados entre los que recibe el usuario, esto permite detectarlos antes de que el usuario acceda a ellos, reduciendo la probabilidad de que un email no deseado llegue al usuario y la posible llegada de un virus dentro de este tipo de email.

¿Cómo se detectan los virus?

Bases de datos de virus conocidos: es la forma clásica de detección de virus, el software tiene una base de datos con los tipos de virus conocidos y su funcionamiento, cuando se analiza un fichero se buscan pequeñas cadenas de datos que son almacenadas en la base de datos de virus. Si se localiza este tipo de cadenas se considera que se ha detectado un virus.

Heurística: la detección heurística nace de la necesidad de detectar los virus de una forma genérica, hasta la creación de los antivirus con detección heurística sólo se podían detectar los tipo de virus conocidos. Lo que suponía ir siempre por detrás de los creadores de virus.

El funcionamiento de la heurística es el siguiente:

1. Desensamblaje del programa

2. Búsqueda de instrucciones sospechosas de pertenecer a un virus. El funcionamiento de este punto suele ser por acumulación de puntos de lo que se considera sospechoso y lo que no, cuando un fichero llega al umbral marcado como detección de un virus salta un aviso y se trata el fichero como si fuera un virus.

3. Se solicita la participación del usuario para decidir qué hacer con el fichero, mostrándole los motivos por los que se sospecha que el fichero está infectado.

Se considera que hay tres tipos de heurística:

- *Genérica*: se buscan similitudes con virus ya conocidos, si un archivo es lo suficientemente parecido a un virus conocidos se considera que es un virus.
- *Pasiva*: se intenta evaluar qué es lo que el software va a hacer, si se considera que el funcionamiento puede ser malicioso se marca como virus.
- *Activa*: el código se ejecuta en un entorno seguro para ver lo que hace, es lo que se conoce como sandbox o virtualización.

El problema de este tipo de detección es que hay una gran probabilidad de tener falsos positivos. Además de que este tipo de análisis puede suponer una carga de cpu que puede afectar al comportamiento del sistema.

¿Qué se hace cuando se detecta un virus?

Hay tres acciones que se pueden hacer cuando un software antivirus detecta la presencia de un virus, la acción más común el eliminar el fichero que contiene el virus, otra opción es ponerlo en cuarentena, es decir, no se elimina pero no se permite el acceso al fichero, por último se puede ignorar el aviso, ya que existe la posibilidad de que sea un falso positivo. Normalmente se deja en manos del usuario la decisión.

5.5. Cifrado de las comunicaciones a través de Internet

Para garantizar las conexiones legítimas a través de una red pública cómo es Internet necesitamos securizar las comunicaciones, y en un medio público la única forma que tenemos es encriptar las conexiones de forma que sean ininteligibles y por tanto inútiles para los posibles atacantes.

5.5.1. Protocolo IPSec (Internet Protocol security):

Es un conjunto de protocolos con la función de securizar las conexiones sobre el Protocolo de Internet (IP). Autenticando y cifrando los paquetes IP. Además, provee de mecanismos para el establecimiento de claves de cifrado.

IPsec actúa en el nivel 3 del modelo OSI (Capa de Red).

IPSec puede funcionar de dos modos:

- **Modo transporte**: sólo la carga útil del paquete IP se cifra y autentica. El resto como el enrutado se mantiene intacto. Se inserta una cabecera AH p ESP entre los datos y la cabecera IP. El datagrama quedaría de la siguiente forma:

IP ORIGINAL	CABECERA AH o ESP	DATOS

Figura 47. Datagrama IP Sec en modo transporte

El modo trasporte se utiliza para conexiones extremo a extremo. Este modo de transporte puede funcionar a través de un NAT transversal. Para que permitir el funcionamiento de IPSec a través de un NAT transversal debemos activar la opción "IPSec Passthrough" en routers domésticos o permitiendo los siguientes protocolos si estamos haciendo uso de un firewall: Internet Key Exchange (IKE) abriendo el puerto 500 de UDP, Encapsulating Security Payload (ESP), abriendo el puerto 50 de IP y si se trata de NAT-T abriendo el puerto 4500 de UDP.

- **Modo túnel**: en este modo todos los paquetes IP y todo su contenido es cifrado y autenticado. Al estar todo cifrado debe ser encapsulado sobre un paquete IP para que funcione el enrutado.

CABECERA NUEVA	CABECERA AH o ESP	CABECERA IP ORIGINAL	DATOS

Figura 48. Datagrama IPSec en modo túnel

Normalmente este modo es usado para interconectar redes con redes (VPN, túneles entre routers, etc), aunque puede ser usado para conexiones extremo a extremo.

La negociación de un túnel IPSec proporciona una conexión segura y cifrada haciendo uso del protocolo IKE. En el procedimiento de conexión se acuerda la seguridad y las claves. Podemos dividir el proceso de conexión en dos partes:

Asegurar la seguridad y la autenticación: para asegurar la seguridad se usa un algoritmo de cifrado simétrico y una firma HMAC[48]. Las claves se intercambian a través del algoritmo Diffie-Hellman. Esta parte finaliza cuando se ha asegurado el canal de comunicación.

[48] Una función MAC (Message Authentication Code) es una porción de información usada para autenticar un mensaje. Los valores se calculan mediante una función HASH con una clave que sólo conocen los dos extremos de la comunicación. HMAC es un tipo de función MAC, que utiliza una función HASH, en la actualidad lo normal es usar SHA-256.

Asegurar la confidencialidad de los datos: con el canal IKE ya establecido se realiza la negociación de parámetros de seguridad específicos IPSec, es decir la cabecera AH o ESP y los algoritmos de autenticación.

A continuación vamos a detallar las cabeceras de seguridad de IPsec de las que hemos estado hablando:

Cabecera AH: proporciona autenticación e integridad de los datos. Para ello como hemos visto utiliza HMAC y calcula la función HASH del paquete mediante el uso de SHA o MD5 y una clave compartida.

Esta cabecera no se cifra y como hemos visto se integra entre la cabecera y la carga útil.

0 -7 bit	8 – 15 bit	16 – 23 bit	24 -31 bit
Next Header	Tamaño Payload	RESERVADO	
SPI (Security Parameters Index)			
Número de secuencia			
HMAC			

Figura 49. Estructura de la cabecera AH usada en IPSec

Next Header: Identifica el protocolo de los datos transferidos

Tamaño de Payload: establece el tamaño del paquete AH

RESERVED: está establecido a 0. Se reserva para futuras implementaciones del protocolo

SPI: identifica los parámetros de seguridad. Estos parámetros se combinan con la dirección IP e identifican la asociación de seguridad implementada.

Número de secuencia: se usa para evitar repeticiones.

HMAC: contiene el valor de verificación de integridad (ICV).

Cabecera ESP: la función principal de ESP es asegurar la confidencialidad de los datos, para ello define el cifrado y la colocación de los datos en el nuevo datagrama IP completo. Posee una estructura más compleja de la de AH que acabamos de ver:

<table>
<tr><th>0 -7 bit</th><th>8 – 15 bit</th><th>16 – 23 bit</th><th>24 -31 bit</th></tr>
<tr><td colspan="4">SPI (Security Parameters Index)</td></tr>
<tr><td colspan="4">Número de secuencia</td></tr>
<tr><td colspan="4">Datos</td></tr>
<tr><td colspan="4">Padding (0-255 bytes)</td></tr>
<tr><td colspan="2"></td><td>Longitud del PAD</td><td>Next Header</td></tr>
<tr><td colspan="4">Datos de Autenticación</td></tr>
</table>

Figura 50. Cabecera de datos ESP utilizada en IPSec

SPI: identifica los parámetros de seguridad. Estos parámetros se combinan con la dirección IP e identifican la asociación de seguridad implementada.

Número de secuencia: se usa para evitar repeticiones.

Datos: los datos que se van a transmitir

Padding: bytes de relleno. Los usan algunos algoritmos criptográficos.

Longitud del PAD: cantidad de datos de relleno.

Next Header: Identifica el protocolo de los datos transferidos

Datos de autenticación: datos usados para la autenticación del paquete.

La parte de datos queda totalmente cifrada, el cifrado de datos se realiza con algoritmos de clave simétrica, normalmente los datos se cifran en bloques, por ello es necesario el uso de bytes de relleno. El algoritmo más utilizado es AES.

La gran ventaja del uso de IPSec es que no es necesario modificar las aplicaciones como ocurre con el uso de otros protocolos.

5.5.2. PGP (Pretty Good Privacy)

Es un software que está pensado para proteger la información que se envía a través de Internet mediante el uso de criptografía de clave pública, en este caso no se cifra el canal si no que es el propio objeto el que se encripta antes de ser enviado.

PGP se considera un sistema de criptografía híbrido, ya que usa una combinación de criptografía de clave pública y de criptografía simétrica.

Cuando un usuario cifra un fichero con PGP, lo primero que se hace es comprimir los datos, esto reduce tiempos en los envíos y en el procesamiento, además añade seguridad criptográfica.

El cifrado se realiza en dos fases:

1. Se crea una clave IDEA[49] o Triple DES aleatoria y se cifran los datos con esta clave.
2. Se cifra la clave IDEA y se envía usando la clave pública RSA del receptor.

El descifrado también se realiza en dos fases:

1. Se descifra la clave IDEA o Triple DES usando la privada de RSA
2. Se descifran los datos con la clave IDEA.

Funcionalidad de PGP:

*Firmar digitalmente y verificar la integridad de mensajes***:** usando RSA y MD5. MD5 condensa el mensaje en 128bit y a continuación se cifran estos 128 bits con RSA.

Cifrar archivos locales: utiliza el algoritmo IDEA o TRIPLE DES.

Generación de claves públicas o privadas: es capaz de generar claves RSA de 512, 768, 1024 y 1280 bits.

Administración de claves: PGP es capaz del envío de claves públicas a los remitentes que posteriormente le van a enviar mensajes cifrados.

Certificación de claves: agrega un sello digital para garantizar la autenticidad de las claves públicas. Es una de las novedades que introdujo PGP ya que se prescinde de una entidad certificadora, basando la confianza en lo que se ha denominado proximidad social.

Revocación, desactivación y registro de claves: PGP es capaz de generar certificados de revocación.

[49] IDEA (International Data Encryption Algorithm) es un algoritmo de cifrado por bloques, estos bloques son de 64bits y se usa una clave de 128bits.

5.5.3. GnuPG

Es una herramienta de cifrado y firma digital similar a PGP, se considera un reemplazo para esta. GnuPG cumple el estándar de la IETF denominado OpenPGP[50] (PGP ha avanzado en sus últimas versiones para cumplir este estándar, pero por el momento no lo cumple completamente). GnuPG está licenciado con licencia GPL por lo que su código es accesible.

GPG utiliza pares de claves asimétricas para cifrar mensajes. Las claves públicas se comparten con el resto de los usuarios, por ejemplo colocándolas en un servidor de claves.

Al igual que en PGP se puede añadir una firma criptográfica a los mensajes, de esta manera la totalidad del mensaje y el remitente puede ser verificado.

GPG no usa algoritmos restringidos por patentes, por lo que no se puede usar el cifrado IDEA presente en PGP. En su lugar es utilizan ElGamal, CAST5, Triple DES, AES y Blowfish. Como algoritmos HASH puede utilizar MD2, MD5, RIPEMD-160, SHA1 (Algoritmo por defecto), SHA256, SHA-384 y SHA512.

Para la compresión se usan algoritmos ZIP y ZLIB.

GPG usa un cifrado híbrido que combina el uso de criptografía de claves simétricas por su rapidez y criptografía de claves públicas tal y como está definido en OpenPGP.

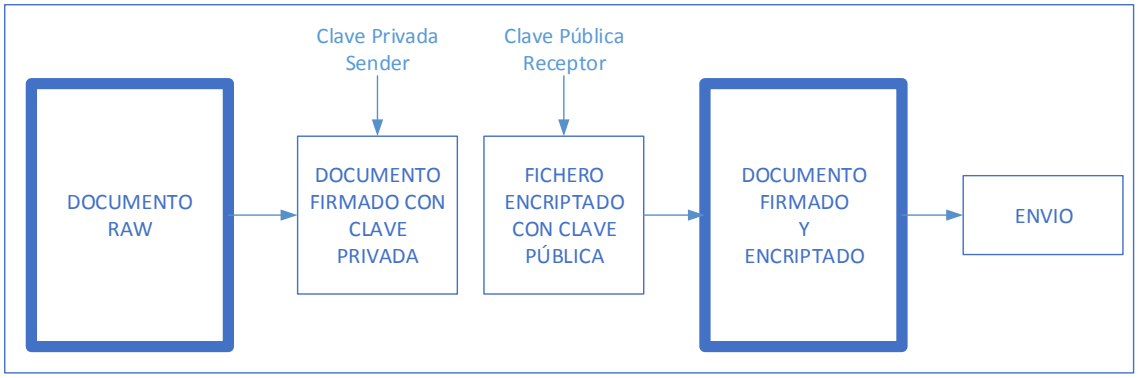

Figura 51. Proceso de envío GnuPG

[50] OpenPGP está definido en la RFC 4880 de la IETF. http://www.ietf.org/rfc/rfc4880.txt de 2007.

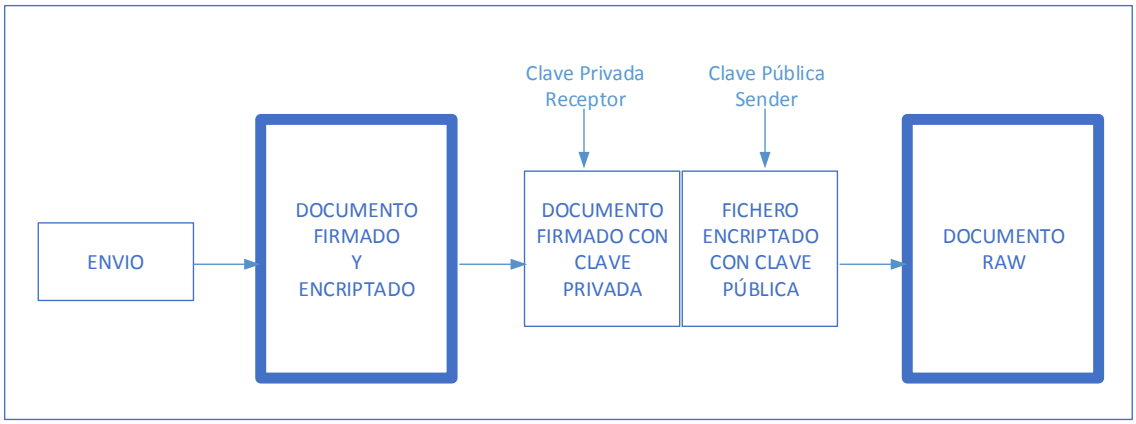

Figura 52. Proceso de Recepción GnuPG

Este tipo de cifra se usa comúnmente en el envío de emails y ficheros.

5.5.4. SSH (Secure SHell)

Es un protocolo de acceso seguro remoto a máquinas que permite el acceso completo a un ordenador. Permite la trasmisión segura sesiones, comandos, passwords, ficheros, etc., sustituyendo por completo sistemas de transmisión inseguros como Telnet o FTP.

Su seguridad reside en el uso de cifrado que hace que la información viaje de forma ilegible.

Como funciona SSH:

1. El cliente envía al servidor una petición al puerto SSH (Por defecto el 22, aunque es configurable).
2. El servidor acepta la conexión y le envía su clave pública al cliente para que este sea capaz de entender los mensajes.
3. El cliente recibe la clave

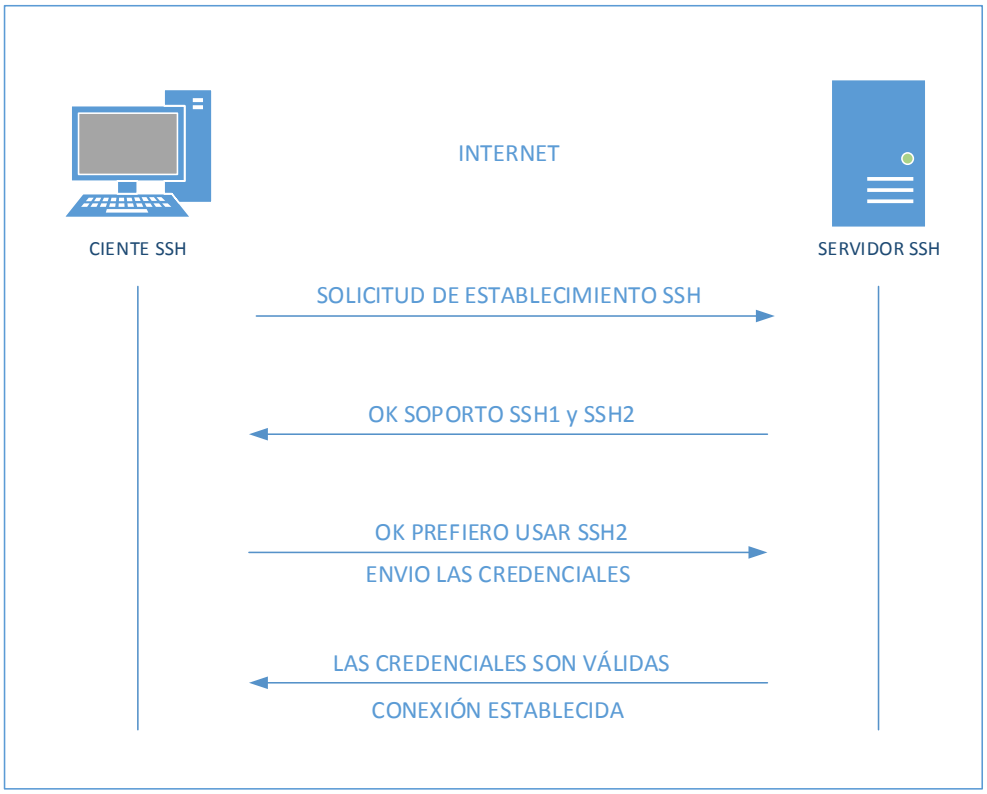

Figura 53. Resumen del proceso de conexión SSH

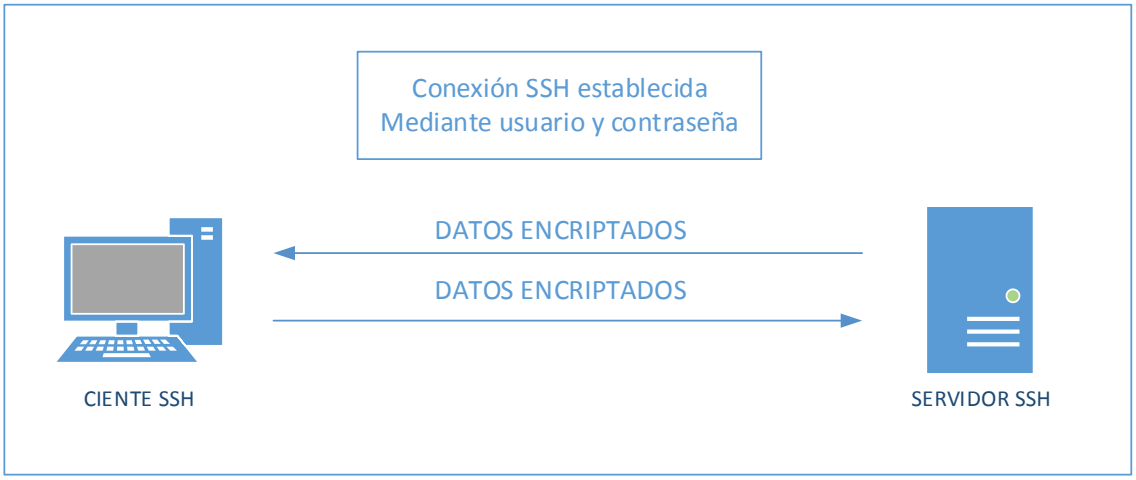

Figura 54. Esquema SSH una vez realizada la conexión

El protocolo SSH tiene la siguiente pila de protocolos:

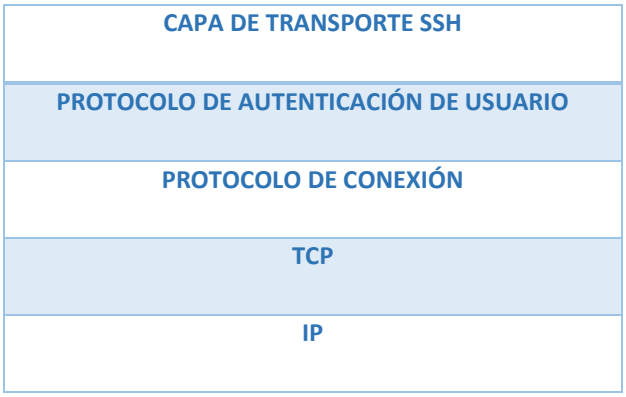

Figura 55. Pila de protocolos SSH

- **La capa de transporte SSH (SSH- TRANS):** se encarga de la autenticación de servidor, de la privacidad, de la integridad y de la compresión. Es responsable del intercambio de claves, configura la encriptación y asigna un identificador único de la conexión.
- **La capa de autenticación de usuario (SSH-USERAUTH):** se encarga de la autenticación de usuario. Los métodos comunes de autenticación son: password, public key, keyboard-interactive, GSSAPI, SecureID, y PAM.
- **La capa de conexión (SSH-CONNECT):** se encarga de definir los canales, simultanear sesiones, ejecución remota de canales, reenvío de las conexiones X11 y TCP/IP.

Aunque el uso de SSH se considera seguro es importante aumentar la seguridad de los sistemas con SSH abierto, a continuación vemos las más importantes:

- No permitir el acceso directo al usuario administrador de la máquina, sobre todo si este tiene un nombre genérico como el usuario **root** en sistemas unix. En la implementación más usada en la red, OpenSSH es tan fácil como añadir la línea *PermitRootLogin No* en el fichero de configuración.
- Es importante cambiar el puerto por defecto de conexión SSH, evitando así ataques automatizados.
- Usar las últimas versiones del protocolo, ya que la versión SSH-1 se considera vulnerable a un ataque de tipo man-in-the-middle.

- Usar software específicos de detección de ataques por fuerza bruta, es sistemas con SSH es imprescindible el uso de Fali2Ban o DenyHosts. Estos dos sistemas son capaces de detectar a través del número de intentos de login un ataque por fuerza bruta y mitigar las consecuencias normalmente baneando la IP desde que se está haciendo el ataque a través de una modificación de las reglas del firewall del equipo.

5.5.5. SSL (Secure Sockets Layer)

SSL es un protocolo creado para transmitir información de forma segura, las aplicaciones que utilizan SSL deben enviar y recibir las claves de cifrado y la cómo cifrar y enviar los datos ya cifrados. Como vemos se sitúa en la capa de transporte:

Aplicación	**HTTPS, IMAPS, POP3S, SMTPS…**
Transporte	SSL
	TCP
Red	IP

Figura 56. Pila de protocolos SSL

En casi todos los escenarios SSL ha sido sustituido por TLS, que estudiaremos a continuación.

El funcionamiento básico de SSL sigue las siguientes fases:

1. El cliente y el servidor negocian los parámetros de la conexión (handshake). Se decide que se va a usar como clave criptográfica entre RSA, Diffie-Hellman, DSA o Fortezza. También se decide que cifrado simétrico se va a utilizar, entre RC2, RC4, IDEA (International Data Encryption Standard), DES (Data Encryption Estándar), triple DES y AES (Advanced Encryption Standard).

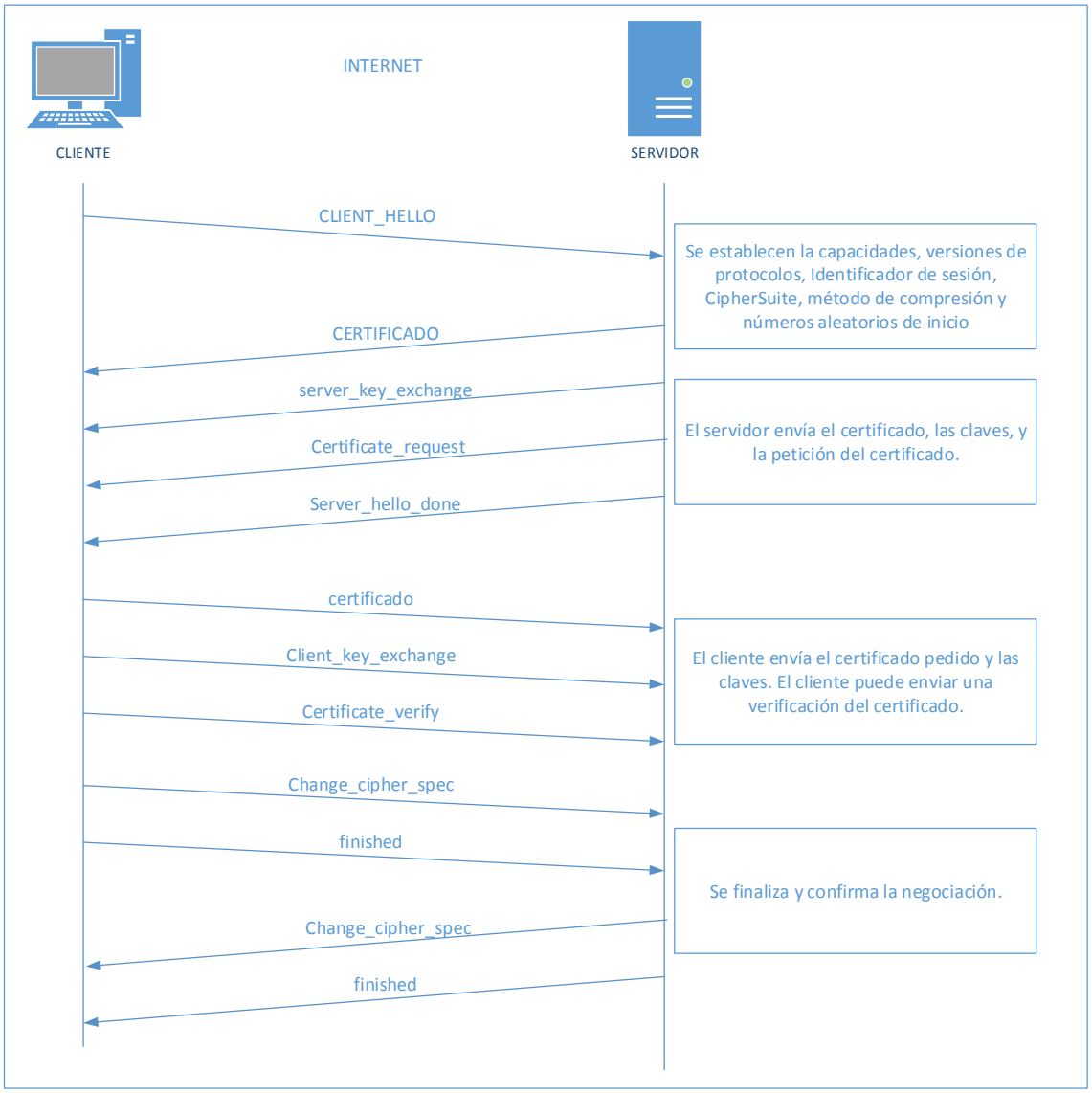

Figura 57. Negociación (Handshake) SSL

CipherSuite es un listado de algoritmos criptográficos soportados por el cliente.

2. Se intercambian las claves públicas y la autenticación basada en certificados digitales.

3. Se usa un cifrado simétrico para el envío del tráfico.

SSL implementa una serie de medidas de seguridad:

- Se numeran los registros y se usa el número de secuencia en el MAC
- Se usa un resumen de mensaje mejorado por una clave sin la cual es imposible verificar el MAC.

- El mensaje *finished* de la negociación SSL incluye una suma de verificación de todos los datos intercambiados.

- El hash divide los datos y utiliza dos métodos distintos, por un lado MD5 y por otro SHA protegiéndose contra una vulnerabilidad puntual de uno de los dos algoritmos de verificación.

5.5.6. TLS

La versión 1.0 de TLS es conocida en la algunos casos como versión 3.1 de SSL, como hemos visto las diferencias son mínimas, las distintas versiones de TLS han sido publicadas por la IETF[51], por lo que podemos encontrar RFC de cada versión que nos detallan su funcionamiento. El desarrollo y documentación de SSL lo realiza la empresa Netscape, lo que hace difícil comparar entre los dos protocolos. TLS versión 1.0 es retrocompatible con SSL versión 3.0, pero trabajando en un modo específico que se considera que reduce la seguridad.

Como vemos la pila de protocolos es idéntica a la de SSL, aunque la propia capa de TLS la dividimos en dos niveles:

<table>
<tr><td>Aplicación</td><td colspan="3">HTTPS, IMAPS, POP3S, SMTPS…</td></tr>
<tr><td rowspan="3">Transporte</td><td>TLS HANDSHAKE PROTOCOL</td><td>TLS CHANGE CIPHERSPEC PROTOCOL</td><td>TLS ALERT PROTOCOL</td></tr>
<tr><td colspan="3">TLS RECORD PROTOCOL</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td>Red</td><td colspan="3">IP</td></tr>
</table>

Figura 58. Pila de protocolos TLS

[51] La IETF (Internet Engineering Task Force) es una organización internacional de normalización, es la encargada de regular los estándares de Internet. Que publica en forma de RFC.

Como vemos en la pila de protocolos podemos dividir la capa TLS en dos capas, la primera conocida como capa de negociación incluye el conocido como protocolo TLS HANDSHAKE, el protocolo TLS CHANGE CIPHERSPEC y el protocolo de alerta: TLS ALERT PROTOCOL. La otra capa sería la capa de registro, que incluye el TLS RECORD PROTOCOL.

A continuación vemos la función de cada uno de estas capas:

Capa de negociación: esta capa está dividida como hemos visto en tres sub-protocolos:

Handshake: este sub-protocolo se usa para negociar la información de sesión entre el cliente y el servidor. Se negocian los siguientes parámetros: ID de sesión, certificados, cipherspec, el algortimo de compresión y un "secreto compartido" que es usado para generar las claves.

Change Cipher Spec: es usado para cambiar el material clave usado para la encriptación entre el cliente y el servidor. El material clave son datos que son usados para uso criptográfico. El protocolo consiste en un único mensaje que indica a la otra parte en la sesión TLS cuál es el par conocido que el remitente quiere cambiar por un nuevo conjunto de claves. La clave se calcula a través de la información intercambiada por el sub-protocolo handshake.

Alert: los mensajes de alerta son usados para indicar un estado o un error. Hay una gran variedad de mensajes para indicar condiciones normales o de error[52]. Normalmente se usan cuando se recibe un mensaje inválido, un mensaje no puede ser desencriptado o el usuario cancela una operación o la conexión se ha cerrado.

Capa de registro: esta capa se apoya en el protocolo TCP. Recibe y encripta los datos que llegan desde la capa de aplicación y envía los datos encriptados a la capa inferior (TCP). El funcionamiento consiste en coger fragmentos de datos del tamaño adecuado al algoritmo criptográfico, de forma opcional puede actuar comprimiendo o descomprimiendo los datos, usa MAC o HMAC. (SSL funciona de forma similar pero no puede funcionar con HMAC). Para encriptar o desencriptar utiliza los parámetros negociados en la fase de negociación. Como resultado de todo esto tenemos una conexión privada y fiable.

Los **objetivos** de TLS son: dotar a la comunicación de seguridad criptográfica, interoperabilidad (las aplicaciones intercambian parámetros sin conocer su el código fuente de la otra), extensibilidad (se pueden añadir nuevos elementos criptográficos) y eficiencia (los algoritmos

[52] Se puede consultar la lista de mensajes completa en la RFC 2246 "The TLS Protocol Version 1.0."

son costosos en cuanto uso de procesador, por lo que se mantiene un caché de sesiones que evita estar continuamente renegociando).

Podemos hablar de tres fases en el funcionamiento de TLS:

1. **Negociación**: los dos extremos negocian los algoritmos criptográficos que van a usar. En TLS se pueden elegir para clave pública entre RSA, Diffie-Hellman, y DSA. Como vemos desaparece Fortezza respecto a SSL. Para el cifrado simétrico Se puede usar RC2, RC4, IDEA (International Data Encryption Standard), DES (Data Encryption Estándar), triple DES y AES (Advanced Encryption Standard). Exactamente los mismo que en SSL. Para las funciones de hash se utiliza MD5 y la familia SHA.

2. **Autenticación y claves**: se realiza la autenticación con el intercambio de certificados digitales X.509[53] y claves de cifrado que se han seleccionado en la negociación.

3. **Transmisión**: la transmisión de datos se considera segura y autenticada.

[53] X.509 es un estándar de la UIT-T para infraestructuras de clave pública (PKI). Especifica los formatos estándar para certificados de calves públicas y el algoritmo de validación de la ruta de certificación. La sintaxis empleada es la propia del lenguaje ASN.1 y los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail).

Detalle del proceso de negociación:

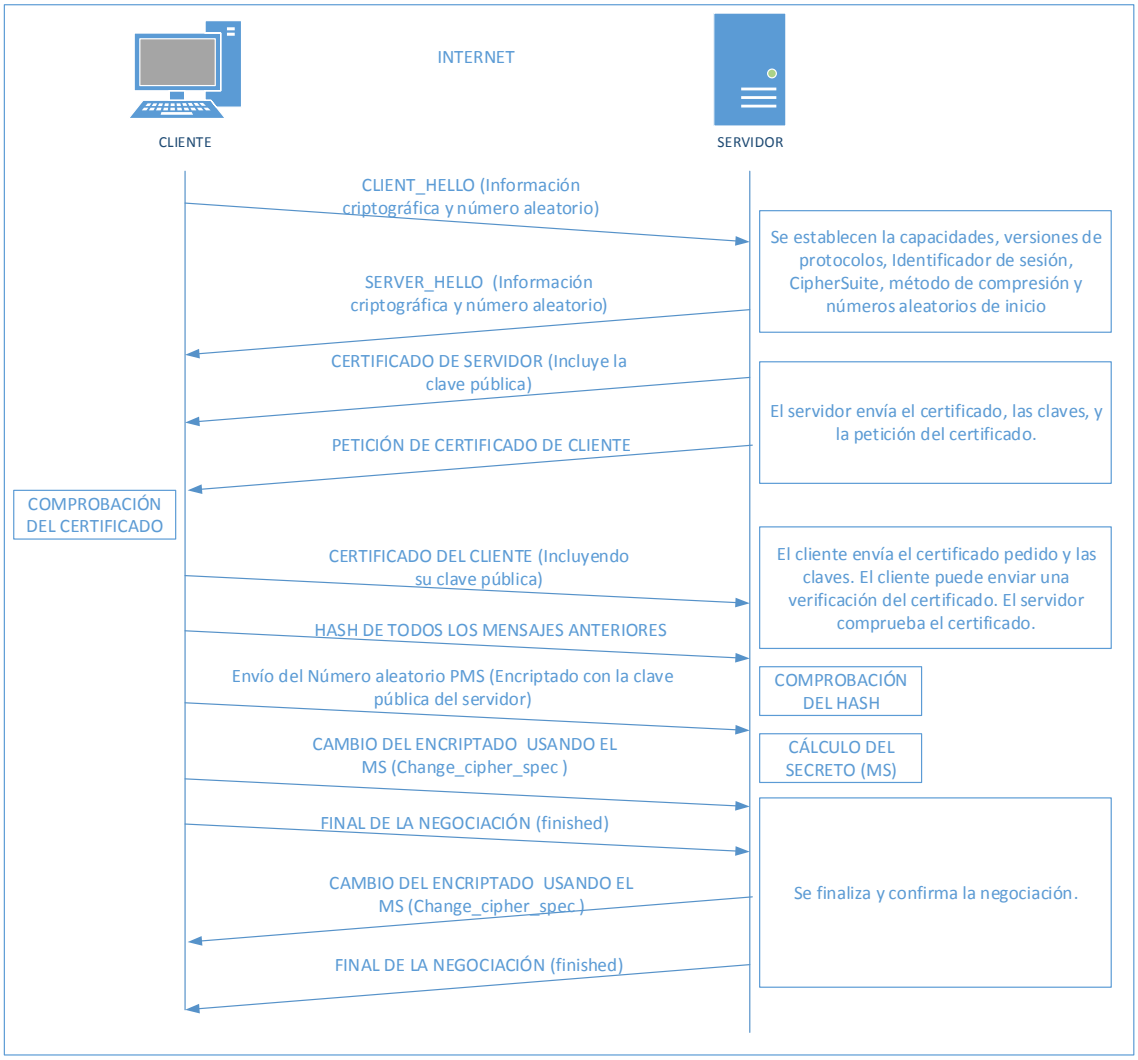

Figura 59. Negociación TLS

TLS implementa una serie de medidas de seguridad para mitigar los posibles ataques, estas medidas de seguridad son similares a las usadas por SSL versión 3.0

- Se numeran los registros y se usa el número de secuencia en el MAC
- Se usa un resumen de mensaje mejorado por una clave sin la cual es imposible verificar el MAC.
- El mensaje *finished* de la negociación SSL incluye una suma de verificación de todos los datos intercambiados.

- El hash divide los datos y utiliza dos métodos distintos, por un lado MD5 y por otro SHA protegiéndose contra una vulnerabilidad puntual de uno de los dos algoritmos de verificación.

5.5.7. VPN

Las redes de las empresas suelen estar protegidas detrás de Firewalls, IDS, IPS y no están expuesta a Internet, por lo menos no del todo, pero en muchas ocasiones los empleados que se encuentran en otras sedes o que realizan el trabajo desde sus casas. Para estos supuestos se utilizan las redes privadas virtuales, VPN. Una red privada virtual es lo que se conoce como un protocolo de túnel, es decir los datos se encapsulan y son enviados cifrados de forma segura a través de Internet. Para los usuarios el funcionamiento es similar al de estar trabajando en la misma oficina (excepto la velocidad ya que depende de la conexión a Internet y de los procesos que lleva a cabo la VPN).

Las VPN sustituyen a las líneas dedicadas, ya que la mayoría de las empresas no se las pueden permitir no es posible utilizarlas desde nuevas ubicaciones con tanta facilidad.

Las VPN se pueden implementar en distintos niveles del modelo OSI:

Implementaciones de la capa de enlace: al encapsular a este nivel se permiten las encapsulaciones no IP, como IPX4. En teoría se puede meter por el túnel cualquier tipo de paquetes. Hay varias tecnologías que implementan túneles a este nivel:

- **PPTP**[54] (Pint to Point Tunneling Protocol): es una extensión del protocolo PPP, fue desarrollada por el PPTP forum. Permite el intercambio seguro de datos entre un cliente y un servidor. La tecnología de PPTP encapsula los paquetes PPP en datagramas IP para transmitirlos por Internet. Sólo es capaz de tener una conexión a través del túnel.

- **L2F** (Layer 2 Forwarding): desarrollado por Cisco, es similar a PPTP, la principal diferencia es que para el establecimiento no depende de IP, es capaz de trabajar directamente con Frame Relay o ATM. Igual que PPTP utiliza PPP para la autenticación

[54] Las especificaciones de PPTP están disponibles en la RFC 2637 de 1999. http://tools.ietf.org/html/rfc2637

del usuario remoto, pero puede utilizar otros sistemas como TACACS+ o radius. Permite más de una conexión a través del túnel.

- **L2TP**[55] (Layer 2 Tunneling Protocol): se ha convertido prácticamente en el estándar de la industria. Al no usar mecanismos de seguridad, debe ser combinada con otros mecanismos de nivel 3. L2TP es una variación de un encapsulamiento del protocolo IP., Un túnel se crea ecapsulando en un paquete UDP una trama L2TP, que a su vez se encapsula sobre IP. Puede ser usado sobre IPSec para proteger la información del túnel.

Implementaciones de la capa de red: IPSec es la tecnología más aceptada a este nivel. Se utilizan dos métodos de IPSec:

- *Modo túnel*: todos los paquetes se encapsulan y son enviados a través del túnel, siendo desempaquetados en el otro extremo. En este modo se protegen las direcciones origen del emisor y el receptor.

- *Modo transporte*: sólo la carga útil es cifrada y encapsulada. La sobrecarga es menor que en el modo túnel. Se exponen los metadatos de los ficheros.

Implementaciones de la capa de aplicación: es posible establecer túneles a nivel de la capa de aplicación. Es usuario puede acceder a la VPN a través de un navegador que se conecta a un sitio web seguro (HTTPS).

Implementaciones multinivel: hay soluciones como OpenVPN que implementa conexiones en las capas 2 o 3, usa TLS para el cifrado y combina todas las características de las anteriores aplicaciones de nivel 2 y 3 que hemos visto.

Es el estándar de la industria cuando hablamos de sistemas basados en Linux.

Puede funcionar en dos modos:

- Basado en claves estáticas precompartidas

- Basado en TLS usando certificados y claves RSA. (Esta opción se considera más segura).

[55] Las especificaciones están disponibles en la RFC 2661 del IETF. http://tools.ietf.org/html/rfc2661

5.5.8. HTTPS

Uno de los puntos más vulnerables y accesibles para los ciberdelincuentes son las páginas web. Aunque se lleva mucho tiempo usando en páginas como las de los bancos, hay una corriente en los últimos años que sugiere que todas las páginas deben ir cifradas, por lo que se desaconseja el uso de http y la sustitución de este por HTTPS.

Para securizar el protocolo HTTP se utiliza SSL (Security Sockets Layer) y su sucesor TLS (Transport Layer Security) que acabamos de conocer.

HTTPS (Hypertext Transfer Protocol Secure) es un protocolo de aplicación basado en HTTP, a través del uso de SSL/TLS crea un canal cifrado que se negocia en el momento de la conexión. Su objetivo es evitar que se intercepten las comunicaciones, o mejor dicho, que si estas son interceptadas no sean inteligibles.

Lo primero que se necesita para configurar un servidor para que acepte conexiones HTTPS es tener un certificado de clave pública, es conveniente que este esté certificado por una entidad certificadora para asegurar la autenticidad. A continuación vemos un esquema simplificado de cómo funciona HTTP:

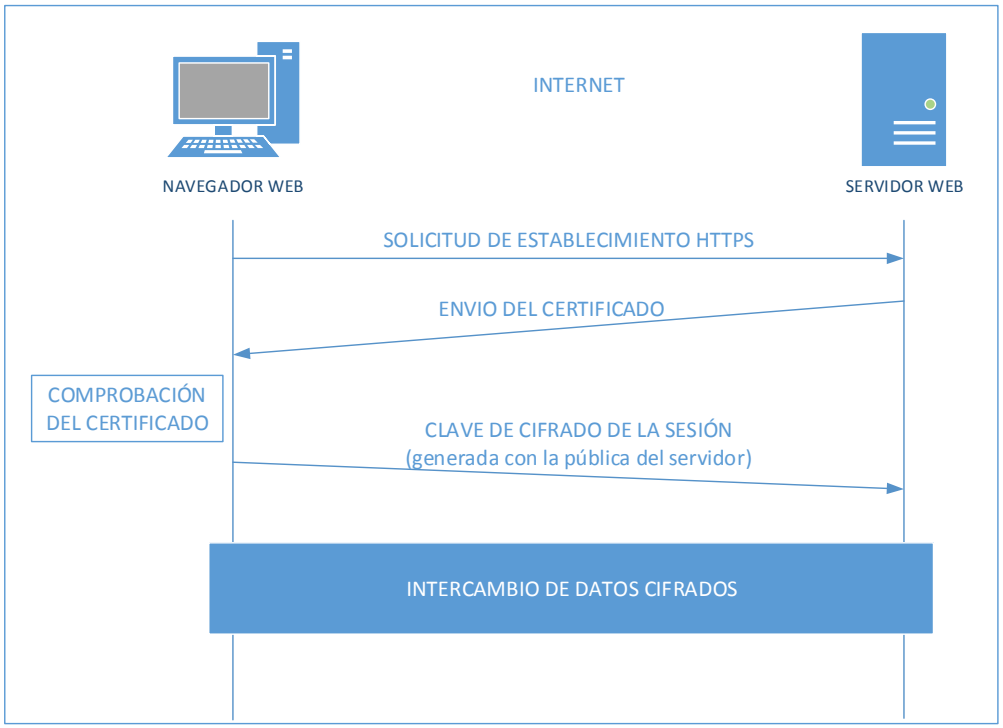

Figura 60. Funcionamiento de HTTPS

Por defecto las conexiones https utilizan el puerto 443.

Pila de protocolos HTTPS:

Aplicación	**HTTPS**
Transporte	SSL/TLS
	TCP
Red	IP

Figura 61. Pila de protocolos HTTPS

5.6. Uso de Software Libre

Aunque no es una técnica como tal, la recomendación de usar software libre es cada más importante si queremos evitar ser atacados o espiados.

A diferencia del software propietario que entrega en forma de binario, sin acceso al código fuente, el software libre distribuye el código del software, lo que permite un auditoría del software, ya que en muchos casos uno de los problemas de seguridad en la inclusión de puertas traseras por los propios programadores.

Los principales proyectos de software utilizan ellos mismos este tipo de auditorías, es el caso del Kernel de Linux, Apache o la distribución OpenBSD.

Otro de los motivos para usar software libre como método de seguridad es no depender de terceros para subsanar fallos de seguridad, ya que en ocasiones grandes empresas de software propietario ignoran fallos conocidos o de dejan de dar soporte a determinadas versiones.

5.7. Protección de la autenticación

Uno de los delitos que como hemos visto contempla en convenio de Budapest y gran cantidad de jurisdicciones es el acceso ilícito a los sistemas.

Hay muchas formas de acceder a equipos de forma ilícita, normalmente este tipo de accesos se hacen a través de ataques por fuerza bruta, ingeniería social o a través de vulnerabilidades.

Ataque por fuerza bruta: un ataque por bruta es tan sencillo o tan complicado como probar todas las combinaciones posibles hasta dar con la contraseña de acceso. Este tipo de ataque

tienen un gran coste computacional, normalmente se combinan con ataques por diccionario, es decir ataques que van probando por fuerza bruta palabras previamente establecidas.

Cuando hablamos de autenticación de usuario tenemos que hablar del protocolo AAA. Estas siglas se corresponden con las de Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting en inglés).

Autenticación: es el proceso por el que un actor prueba su identidad a una entidad. La autenticación se consigue mediante la presentación de la identidad, por ejemplo un nombre de usuario, y la presentación de las credenciales que la corroboran, como puede ser la contraseña, un certificado o una clave.

Los métodos de autenticación se dividen en tres categorías:

- Basados en algo previamente compartido, como puede ser una contraseña o un passphrase.
- Basados en algo poseído, como puede ser una tarjeta de identificación o un DNI electrónico.
- Basados en las características físicas del usuario, como puede ser una huella dactilar o la forma del ojo.

En los últimos años se han impuesto los sistemas de doble factor de autenticación para mejorar la seguridad de los sistemas. Este tipo de sistemas mezclan los tipos basado en algo previamente poseído con algo poseído, esto último se envía de forma dinámica en el momento que se produce el primer intercambio.

El ejemplo más común es el envío de un token al teléfono móvil o al correo electrónico en el momento que se introduce un usuario y contraseña válidos. No se produce la autenticación hasta que no se introduce este token. Normalmente este tipo de token tiene un tiempo de vida limitado.

Autorización: se refiere a los privilegios que se otorgan a un usuario a través de su identidad, generalmente su nombre de usuario.

Contabilización: monitoriza el consumo de los recursos de red de un usuario, esta información puede usarse para muchos propósitos como la facturación posterior.

5.8. Sistemas AntiSpam

Se conoce por correo basura o SPAM al envío de correos electrónicos no deseados, este tipo de correos normalmente se utiliza para el envío de publicidad no deseada (si la publicidad es aceptada como el envío de un newsletter aunque el envío sea masivo no se considera SPAM), aunque no es lo único que llega con este tipo de mensajes, ya que en muchas ocasiones se utilizan para el envío de virus, timos, phising…).

El envío de SPAM es un problema a nivel mundial, en la siguiente gráfica vemos los principales países emisores de SPAM:

Figura 62. Principales países emisores de SPAM. (33)

En muchos casos se utiliza una dirección de correo falsa par este tipo de envíos, lo que se conoce como suplantación de correo electrónico o mail spoofing. Este tipo de suplantación es muy sencilla de hacer, ya que sólo se necesita un servidor SMTP, la única forma de comprobar que el remitente es quien es comprobar que el dominio y la IP del remitente se corresponden.

Para conseguir las direcciones de correo electrónico los "spammers" rastrean las web públicas buscando direcciones, cogen las direcciones de los mensajes de los grupos de noticias, las listas de correo, las cadenas de correo electrónico, etc.

(33) **Sophos.** España se mantiene en el Top Ten de países emisores de correo basura. [En línea] 2014. http://sophosiberia.es/espana-se-mantiene-en-el-top-ten-de-paises-emisores-de-correo-basura/.

Una vez que tienen suficientes direcciones se realizan los envíos, ya sea desde sus propios servidores o desde servidores que han sido víctimas de un acceso ilícito. También es posible enviar correos desde otros servidores utilizando las funciones de relay si existe una mala configuración de seguridad.

Por sistema antispam se conoce a los métodos para detectar y eliminar el correo basura.

Aunque hay muchos sistemas antispam a nivel usuario, la mayoría del correo basura se elimina antes de llegar al usuario, son los conocidos como antispam de administrador, este tipo de antispam hace una serie de comprobaciones sobre cada correo electrónico recibido:

Listas de bloqueo: una de las primeras comprobaciones que hace un sistema antispam cuando recibe un correo electrónico, es comprobar que la IP de origen no se encuentra en este tipo de lista negra. Si el dominio / dirección IP (entre los equipos bloqueados en normal encontrar equipos que han sido infectados por algún virus y que ha sido utilizado para el envío de SPAM) se encuentra en las lista el mensaje será marcado como spam o desechado en función de la configuración. Hay multitud de listas públicas de bloqueo en internet, como la de Spamhaus, uribl o Cisco.

SPF: SPF una extensión del estándar SMTP, creado para comprobar que una dirección de correo no ha sido falsificada, para ello se identifica a través de los nombres de dominio de los servidores SMTP que están autorizados para envío de correo.

Configurar el DNS para SPF es muy sencillo si eres el usuario legítimo. Una entrada de registro DNS quedaría de la siguiente forma:

Dominio.es IN TXT “v=spf1 ptr ~all"

Donde v define la versión de spf usada, mx son las máquinas autorizadas, con ptr se autoriza a las máquinas bajo el mismo dominio y con ~all se desautoriza al resto.

Filtrado de contenido: se analiza el contenido del mensaje buscando palabras clave, si se produce un número predeterminado de coincidencias con las palabras buscadas el email e considera correo no deseado.

Filtrado mediante resolución inversa: otra de las comprobaciones que realizan la mayoría de los sistemas antispam es lo que se conoce como resolución inversa. Para determinar la veracidad del dominio que remite el mensaje se hace una petición de resolución DNS inversa,

es decir a través de la IP sabemos el dominio. Para que la resolución inversa funcione hay que añadir la entrada PTR al registro DNS.

Existencia de registro MX: es un tipo de registro DNS que especifica cómo debe ser recibido un email. El registro MX apunta a los servidores a los que se envía un correo electrónico y establece la prioridad en caso de haber varios. Un mismo registro DNS puede tener varios valores MX, el de mayor prioridad será el que tenga un valor MX menor. Lo normal es que el sistema antispam tenga mayor prioridad que el servidor de correo para que los correos pasen antes por el antispam que por el servidor de correo. Para la detección de SPAM se comprueba que exista al menos un registro MX en el servidor que ha enviado el correo.

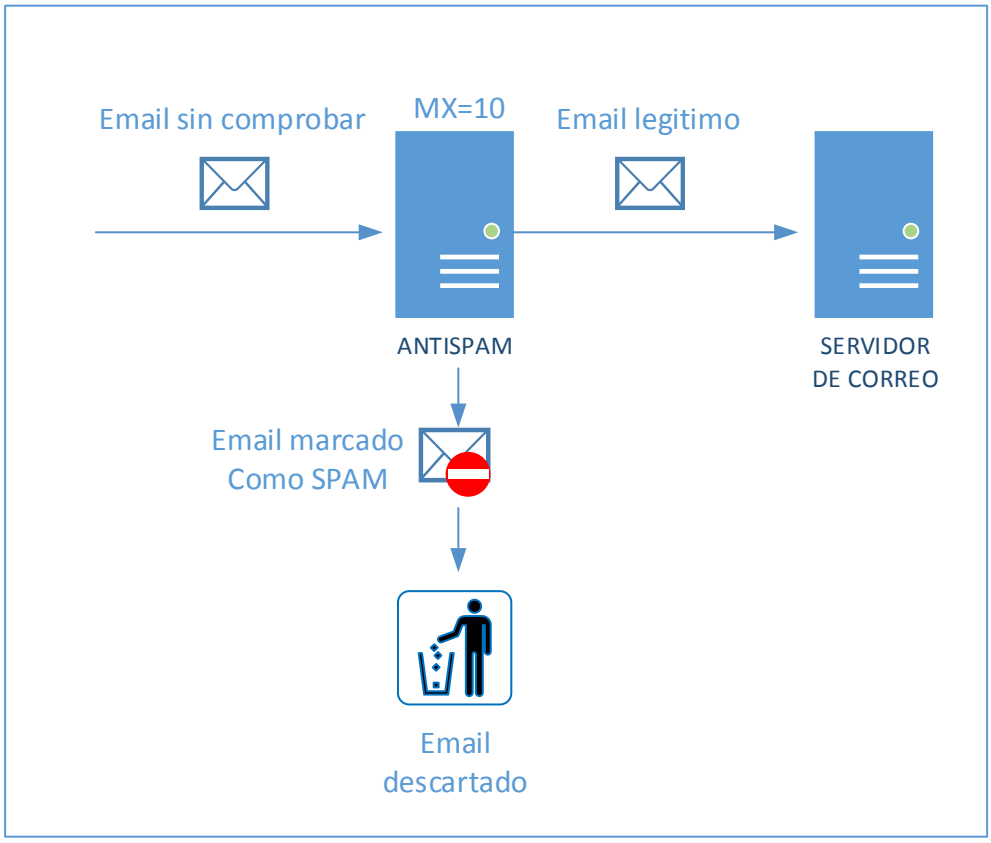

Figura 63. Esquema de conexión antispam.

Como hemos comentado los emails los recibe el servidor con menor MX, a continuación hace las comprobaciones que hemos comentado y decide si descarta el email o lo pasa al servidor de correo.

5.9. Auditorías de Seguridad

Aunque no es una herramienta como tal, al menos no una herramienta software, a nivel empresarial es prácticamente imprescindible el uso de este tipo de auditorías que permiten a las empresas anticiparse a posibles ataques. Además este tipo de auditorías se deben realizar periódicamente o continuamente, porque dejan de ser válidas casi en el momento de realizarse, ya que pueden aparecer nuevas vulnerabilidades en cualquier momento.

Tipos de auditorías de seguridad:

- **Interna**: el auditor asume el rol de un usuario con acceso a los sistemas de la empresa. Este tipo de auditoría intenta detectar las vulnerabilidades en servidores internos, en las comunicaciones de la red corporativa, configuraciones erróneas, sistemas sin actualizar, WIFIs inseguras, etc.

- **Seguridad perimetral:** permite conocer lo que un atacante externo puede llegar a hacer y si es capaz de acceder a los sistemas internos, se busca sacar a la luz las vulnerabilidades técnicas, las consecuencias que tendrían en el caso de que alguien las aprovechase y lo que habría que hacer para evitar los riesgos.

- **Test de intrusión (pen test)**: consiste en la simulación de un ataque real contra los sistemas de la empresa, de esta forma se determina el nivel de seguridad y el grado de acceso al que puede llegar un atacante. Hay tres subtipos de test de intrusión:

    - **Caja Negra:** el auditor no tiene conocimiento ninguno de los sistemas a revisar.

    - **Caja Blanca:** el auditor tiene conocimiento de los sistemas: sistemas operativos, software, arquitectura, etc.

    - **Caja Gris:** el auditor simula la posición de un empleado que dispone de cierta información como puede ser un usuario sin privilegios. Se buscan vulnerabilidades que permitan escalar los privilegios.

- **Análisis Forense:** este tipo de análisis se produce después de que se haya producido un incidente de seguridad, intenta explicar que ha pasado, quien ha realizado el ataque, cómo ha realizado el ataque y que ha comprometido la persona o máquina que ha realizado el ataque.

- **Auditoría de páginas web**: se analiza la parte externa de la web (o webs) de la empresa, comprobando si existen vulnerabilidades (inyección de código SQL, cross site scripting, etc.) y que ocurriría si un atacante intenta aprovecharse de ellas.

- **Auditorías de código de aplicaciones**: este tipo de auditoría se debe realizar en el proceso de desarrollo del software. Con este tipo de auditoría se buscan vulnerabilidades, pero también sirve para fomentar buenas prácticas de programación.

CAPÍTULO 6.CONCLUSIONES

6. Conclusiones

Vivimos en lo que se conoce como la sociedad de la información, el intercambio de información es lo que dio origen a la red, y es el objeto de los ciberdelincuentes, proteger este intercambio es de vital importancia. Cada vía más el mundo se globaliza y es gracias a la tecnología y su espectacular avance en los últimos años, este avance se antoja imparable y con él la interconexión de las personas, empresas, gobiernos y todo tipo de organismos. Esto hace que los delitos que se cometen en, o través del a red sean cada vez más y más importantes.

La complejidad y la idiosincrasia de la red de redes hacen que los ciberdelitos sean complejísimos de perseguir, la ubicuidad de la red hace posible que se den casos en los que el caso perseguido sea delito en un país pero no en otro, o que la sentencia condenatoria de un país quede inejecutada porque otro país no ejecute una norma penal extranjera.

En los últimos años se ha avanzado mucho en la colaboración entre los estados y esta colaboración es la clave de la lucha contra la ciberdelincuencia, el Convenio de Budapest es a día de hoy la referencia mundial a la hora de legislar los ciberdelitos, pero la rapidez de crecimiento y evolución del ciberdelito hace que tengan que ser revisados los delitos que este define.

Los delincuentes cada vez cuentan con sistemas más avanzados que les permiten ocultarse en la red, herramientas como las conocidas como redes oscuras son cada vez más fáciles de usar, lo que hace que los delitos sean cometidos sean cometidos también por personas sin conocimientos técnicos que cada vez tienen más fácil cometer un delito.

La defensa contra los delitos informáticos cada vez es más compleja, aunque el uso de sistemas como los firewalls sigue totalmente vigente, cada vez son necesarios nuevos sistemas que consigan mantener los sistemas fuera del alcance de intrusos, los conocidos como sistemas de detección y prevención de intrusiones cada vez son más necesarios.

Los datos son en este momento fuente de negocio, que se espera que vaya en aumento en los próximos años, cada vez es más necesario proteger nuestras comunicaciones, esto se consigue cuando hablamos de Internet casi en exclusiva con la encriptación de los datos, el uso de protocolos sin cifrar como http cada vez más caen en desuso a favor de los sistemas similares cifrados (https en este caso). Esta encriptación se hace a distintos niveles, desde proteger un dato en concreto (GPG y PGP) a proteger toda una comunicación completa (con el uso de

protocolos de transporte como IPSec o con la creación de túneles por los que se transmita la comunicación (VPN, TLS, SSH, etc.).

Cada vez la penetración de Internet es mayor, esto hace que gran parte de la población mundial está conectada, muchas de estas personas sin la suficiente formación y pericia en el uso de la red y lo que puede encontrar en ella. Esto hace que las imprudencias y el mal uso faciliten también la labor de los delincuentes.

El uso de comunicaciones inalámbricas y la telefonía móvil añaden vulnerabilidades propias del acceso al medio físico en el que se realiza la comunicación.

Cualquier investigación sobre el ciberdelito nos hace ver que cada día el cibercrimen crece y que los sistemas son vulnerables, da la impresión de que cualquier sistema puede ser atacado con éxito, si un sistema es objeto de un ataque dirigido es prácticamente imposible una defensa efectiva. Hasta los servicios de inteligencia como la NSA estadounidense han sido atacados.

Con la lucha contra el cibercrimen surgen problemas para conciliar la lucha con la protección de la intimidad de las personas, muchas leyes de protección de datos y convenios en la materia chocan con los comportamientos de los gobiernos.

CAPÍTULO 7. BIBLIOGRAFÍA

7. Bibliografía

1. *Los cibercrímenes en el espacio de libertad, seguridad y justicia.* **Bernal, Antonio Pedro Rodríguez.** s.l. : Alfa-Redi, 2006, Revista de derecho informático Alfa-Redi.

2. **Unión Internacional de Telecomunicaciones.** *Guía de Ciberseguridad para los Paises en Desarrollo.* [http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf] 2007.

3. **Europa, Consejo de.** Convenio Europeo de Ciberdelincuencia. Budapest : s.n., 2001.

4. —. *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.* 2013. 261/05/CON.

5. **El Banco Mundial.** El Banco Mundial BIRF-AIF. *Usuarios de Internet (por cada 100 personas).* [En línea] 2013. http://datos.bancomundial.org/indicador/IT.NET.USER.P2/countries?page=2&display=map.

6. **Norton Symantec.** *Informe sobre el cibercrimen Norton.* 2011.

7. **United Nations Office on Drugs and Crime.** *Comprehensive Study on Cybercrime.* Viena : s.n., 2013. UNODC CCPCJ EG.4.

8. **Unicef.** *Seguridad infantil en Internet: retos y estrategias mundiales.* 2011.

9. **INTECO.** *El ministro de Industria, Energía y Turismo presenta una campaña contra el ciberacoso infantil.* 2013.

10. **Observatorio ABACO.** Penetración de internet (empresas). [En línea] http://www.observatorioabaco.es/post_observatorio/penetracion-de-internet-empresas.

11. **Clarke, Richard A.** *Guerra en la Red. Los Nuevos Campos de Batalla.* Barcelona : Ariel, 2011. ISBN 9788434469600.

12. **Nakashima, Ellen.** The Washington Post. *Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies.* [En línea] 27 de Mayo de 2013. http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

13. **Diez, Javier A.** Perfil de un Hacker. [En línea] http://www.derechopenal.unican.es/contenido/hackers.pdf.

14. **Interpol.** Interpol. *El Complejo Mundial de INTERPOL para la Innovación.* [En línea] 2014. [Citado el:] http://www.interpol.int/es/Acerca-de-INTERPOL/El-Complejo-Mundial-de-INTERPOL-para-la-Innovaci%C3%B3n.

15. **Europa, Consejo de.** *Decision 2009/371/JAI.*

16. **Europol, ENISA y.** Comisión Europea. *Lucha contra la cibedelincuencia: ENISA y Europol firman un acuerdo estratégico de cooperación.* [En línea] 2014. http://ec.europa.eu/spain/pdf/ip270614%282%29.pdf.

17. **Asamblea general de la ONU.** Resolución 55/63. [En línea] http://www.unodc.org/pdf/crime/a_res_55/res5563s.pdf.

18. **OECD, Ministerial session.** OECD.org. *The Seoul Declaration for The Future of the Internet Economy.* [En línea] 2008. http://www.oecd.org/internet/consumer/40839436.pdf.

19. **OAE.** Portal Interamericano de Cooperación en materia de Delito Cibernético. [En línea] http://www.oas.org/juridico/spanish/cybersp.htm.

20. **OTAN.** NATO and cyber defence. [En línea] 2014. http://www.nato.int/cps/en/natolive/topics_78170.htm.

21. **Comisión Europea.** *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Comisión Europea.

22. **Wegener, Henning.** *LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA.* 2014.

23. **Center for Strategic and International Studies.** *Net Losses: Estimating the Global Cost of Cybercrime.* Washington, DC : s.n., 2014.

24. **Nora, Simon y Min, Alain.** *La informatización de la sociedad.* 1977.

25. **Eurojust e Iber-RED.** *Memorandum de Entendimiento entre Eurojust e Iber-RED.* Mayo 2009.

26. **BOE.** *LOPJ.* 1985.

27. **XcepticZP.** commons.wikimedia.org. [En línea] http://commons.wikimedia.org/wiki/File:Freenet_Request_Sequence_ZP.svg.

28. **LOIC.** Github de LOIC. *Github.* [En línea] http://sourceforge.net/projects/loic/.

29. **amiri, Novan.** Skynet Cyber4RT. *Software HOIC.* [En línea] http://skynetcyber4rt.blogspot.com.es/2014/06/blog-post_182.html.

30. **map, digitalk attack.** Digital Attack Map. *Undertanding DDoS.* [En línea] http://www.digitalattackmap.com/understanding-ddos/.

31. **securitybydefault.** securitybydefault. *Cómo CyberBunker atacó a Spamhaus y casi se llevó a medio Internet por delante.* [En línea] http://www.securitybydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html.

32. **Romero, P.** elmundo.es. *El detenido por el 'ciberataque' a Spamhaus dice ser 'diplomático de la Rep. de Cyberbunker'.* [En línea] http://www.elmundo.es/elmundo/2013/04/28/navegante/1367139728.html.

33. **Sophos.** España se mantiene en el Top Ten de países emisores de correo basura. [En línea] 2014. http://sophosiberia.es/espana-se-mantiene-en-el-top-ten-de-paises-emisores-de-correo-basura/.

34. **Martín, Cristos Velasco San.** *La jurisdisción y competencia sobre delitos cometidos a través de sistemas de computo.* Valencia : Tirant Lo Blanch, 2012. 978-84-9004981-5.

35. **Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman.** *The Darknet and the Future of Content Distribution.* s.l. : Microsoft Corporation, 2002.

36. *La oportunidad criminal en el ciberespacio.* **Llinares, Fernando Miró.** 13-07, Elche : s.n., 2011, Revista Electrónica de Ciencia Penal y Criminología. 1695-0194.

37. *El fenómeno del cibercrimen en Internet y la World Wide Web: una mirada criminológica.* **Sain, Gustavo.** Cuaderno 13, Buenos Aires : Ministerio de Seguridad de Argentina.

38. *Consideraciones sobre el Foro Mundial de Política de las Telecomunicaciones/TIC.* **Unión Internacional de Telecomunicaciones.** Ginebra : s.n., 2013, pág. 1.

39. **Díaz Gomez, Andrés.** *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest.* La Rioja : Universidad de La Rioja, 2011. ISSN 1668-5024.

40. **González, Juan de Dios Meseguer.** *Hacia la compresión psocjurídica de los Ciberdelincuentes y Cibercriminales.*

41. **Europa, Consejo de.** *Convenio 108.*

42. **Instituto Elcano.** Tecnología y defensa. [En línea] http://www.blog.rielcano.org/tecnologia-y-defensa/.

43. **Unión Internacional de Telecomunicaciones.** *El ciberdelito, guía para los países en desarrollo.* 2009.